POL00423454

Audit, Risk and Compliance Committee Agenda

Date:	Monday 25 March 2019	Time	12.30 – 14.40 hrs	Location	1.19 Wakefield

Present	Other Attendees	
• Tim Franklin • Tom Cooper • Ken McCall	• Alisdair Cameron (Group CFOO) • Shirine Khoury-Haq (Non-Executive Director) • Andrew Paynter, PwC (External Audit Partner) • Lucy Mason, PwC (Senior Manager) • Amanda Bowe (item 2) – by telephone (Chair, ARC PO Insurance) • Liz Robson (Change and IT Director – Retail) (item 6.)	• Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Jonathan Hill (Compliance Director) • Veronica Branton (Head of Secretariat) • Rob Houghton (Group CIO) (items 6. & 7.) • Mick Mitchell (IT Security and Service Director) (item 6.)

	Agenda Item	Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest**	Noting	Chair	
2.	**Update from Subsidiaries:** • Post Office Management Services ARC (Verbal)	Noting & Input	Amanda Bowe	12.30 – 12.35
3.	**Minutes and Matters Arising**			
3.1	Minutes of the Audit, Risk and Compliance meeting held on 29 January 2019	Approval	Chair	12.35 – 12.40
3.2	Actions List	Noting & Input		
3.3	Draft Minutes of the Risk and Compliance Committee held on 14 March 2019	Noting		
4.	**Risk**			
4.1	Risk Report	Noting & Input	Jenny Ellwood	12.40 – 13.10
5.	**Compliance**			13.10 – 13.35
5.1	Compliance Report *Including an update on Fit & Proper*	Noting & Input	Jonathan Hill	
5.2	The Fin11 issue and Telecoms Controls	Noting & Input	Colin Stuart	
6.	**Information Security Update** - *Cyber Security* - *Password exposure* - *PCI Compliance* - *Payzone*	Noting & Input	Rob Houghton / Mick Mitchell/ Liz Robson	13.35 – 13.55
7.	**Back Office Transformation**	Noting & Input	Ben Cooke/ Rob Houghton/ Al Cameron	13.55 – 14.05

POL00423454

Audit, Risk and Compliance Committee Agenda

8. 8.1 8.2	**Internal Audit** Internal Audit Report Internal Audit Plan 2019/20	 Noting & Input Approval	Johann Appel	14.05 – 14.30
9.	**Policy Review** Treasury Policy	Approval	Mark Dixon	14.30 – 14.35
10.	**Any other Business** Note: Date of next meeting 21 May 2019, 09.30 – 11.30 hrs	Noting	Chair	14.35 – 14.40

POL00423454

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 TUESDAY 29 JANUARY 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 08.30 AM

Present:	Carla Stent	Chair **(CS)**
	Tim Franklin	Non-Executive Director **(TF)**
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)**
In Attendance:	Paula Vennells	Group Chief Executive **(PV)**
	Alisdair Cameron	Group Chief Financial and Operating Officer **(AC)**
	Tim Parker	Chairman, PO Limited **(TP)**
	Shirine Khoury-Haq	Non-Executive Director **(SK)** (items 5. – 10.)
	Andrew Paynter	Group Audit Partner, PwC **(AP)**
	Lucy Mason	Group Audit Senior Manager, PwC **(LM)**
	Chris Neale	Group Audit Director, PwC **(CN)**
	Stewart Light	Systems and Controls Director, PwC (by telephone) **(SL)**
	Jane MacLeod	Group Director, Legal, Risk and Governance **(JM)**
	Johann Appel	Head of Internal Audit **(JA)**
	Jenny Ellwood	Risk Director **(JE)**
	Jonathan Hill	Compliance Director **(JH)**
	Veronica Branton	Head of Secretariat **(VB)**
	Sally Smith	MLRO **(SM)** (item 6.)
	Rob Houghton	CIO **(RH)** (item 7.)
	Mick Mitchell	IT Security & Service Director **(MM)** (item 7.)
Apologies:	Amanda Bowe	Chair, ARC PO Insurance

ACTION

1. WELCOME AND CONFLICTS OF INTEREST

1.1 The Chair welcomed PwC to the meeting and especially Chris Neale who was attending his first meeting and would be joining two ARC meetings a year to provide an additional perspective, particularly on IT change.

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

2. UPDATE FROM SUBSIDIARIES

Tim Franklin provided an overview of the key issues from recent PO Insurance ARC meetings:

- PO Insurance had commissioned a review of TIF, its travel insurance underwriter, following reports alleging instances of poor treatment of customers. The initial findings of the review were being analysed but the PO Insurance Board wished to look at alternative providers
- the Competition and Markets Authority's (CMA) response to the super complaint lodged by Citizens Advice created a less stable environment for both PO Insurance and Telecoms. It was hard to gauge what the industry's response would need to be but we were monitoring the situation.

It was **AGREED** that the CMA's response to the super complaint should be shown as a potential strategic risk on the risk register. PO Limited had a significant volume of vulnerable customers and customers who were over 65 and these groups were a focus for the regulator. It was confirmed that we had information on the pricing differentials for Telco. **JE**

It was noted that we remained 20% out of tolerance for the quality of sales of financial services products in the branch network. The situation had been notably problematic with some of the multiples like WH Smiths. It was asked whether we should we be taking a different approach in light of this and a request was made for ARC to look at the issue in more depth. It was also suggested that we needed a marginal contribution analysis for the multiples and it was reported **JE**

POL00423454

that this would be included as part of the Retail Strategy paper to the March Board. JH reported that PO was working with BoI on how we engaged with multiples like WH Smiths.

3. MINUTES OF PREVIOUS BOARD AND MATTERS ARISING

The minutes of the meeting of the Audit and Risk Committee held on 30 October 2018 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

4. RISK REPORT

4.1 Jenny Ellwood provided an overview of the key issues from the report and updates since the report had been issued:

- Back Office transformation had gone live on 24 January 2019, when we had migrated from POLSAP onto the new system. AC reported that manual working had been instituted in half a dozen areas, one fix had been implemented and others were in train. The manual interventions required in Supply Chain were manageable. 200 RM Special Deliveries had not been collected on 28 January 2019 but measures were in place to make sure this error was not repeated. Until we starting receiving the cash reconciliations we could not be confident about the success of the migration but the issues identified to date were resolvable
- Brexit and a "no deal" scenario. A range of mitigations had been put in place and since the report had been issued we had spoken with the Bank of England about whether they wanted us to stock more cash in our distribution centres. They did not think this was necessary currently but we had staff ready in the week before and after the exit date should this be required
- we were maintaining a close watching brief on PCI compliance
- emerging risks were going to be a regular section of the Risk Report
- the risk appetite was still in development but a heat map had been included in the Report for the first time
- JE had arranged a meeting with the insurers to identify the risks we were insured against and those we were not.

4.2 A number of points were raised, including:

- whether the Security Strategy Plan was mitigating the risks? JE reported that the residual risk had decreased but that we would be bringing metrics on progress to the March ARC meeting
- what interaction there was with the business when assigning risk ratings? It was reported that the Risk Team assigned a risk rating initially but then discussed this with the business area. CS noted that she wanted to be sure that ARC was getting the view of the second line of defence
- whether Anti Money Laundering (AML) should be listed as a principal risk? It was reported that there was going to be a deep dive on financial crime in February 2019 and the severity of the risk would be considered further at this point. The whole network was required to undertake a number of pieces of training that linked to our AML obligations but the need for further work to strengthen against the AML risk was acknowledged
- our view of the financial stability of multiple partners from a risk perspective? It was reported that we did not have a rating for that presently. TC offered to put JE in touch with colleagues at UKGI/ BEIS who had a watching brief on potential insolvencies — **TC**
- It was **AGREED** that an update would be provided on the EUM project. — **Exec**

JE was commended on the good progress that had been make in developing the Report.

5. COMPLIANCE UPDATE

5.1 **Compliance Report**

Jonathan Hill introduced the report and highlighted the key items:

POL00423454

- that we had decided to self-report to Ofcom our non-compliance over a four year period with the requirement to discount calls for customers using Text relay (this related to hearing impaired customers). Since November 2018, customers using Text relay had been able to make these calls free of charge. 53 customers had used Text relay over the four year period, though only 17 were impacted negatively from a financial perspective. We had not yet heard back from Ofcom formally but anticipated a potential fine in the region of £200k and £400k
- Ofcom complaints for Post Office Home Phone were at their lowest levels to date[1]
- the Security Strategy Plan and the work of the Compliance Team would be coordinated. We were focussed on raising personal accountability and awareness of security issues and expected to see significant improvements in this area.

5.2 A number of points were raised, including:

- why we had not reported the Text relay breach to Ofcom earlier and whether the anticipated fine level was high given the small number of customers affected and its limited impact? While this non-compliance had been known by the Telco team for some time, it had been escalated following the change of leadership and appointment of a Telco compliance manager. As a result of escalation, specialist regulatory advice was sought and the decision taken to self-report. CS noted that she wanted assurance that late reporting or failure to report compliance breaches was not a cultural issue. JH confirmed that there was increasing engagement of the Compliance team with change functions as well as more dedicated compliance resources. Oversight of outsourcers required a different approach and work was underway to embed this from a regulatory perspective
- concerns were expressed about the Compliance Team being overstretched and the difficulty that had been experienced in recruiting suitable candidates. JH reported that one offer had just been made and that an additional compliance professional had recently joined the business. Our Data Protection Officer (DPO) was on long-term sick leave but we had appointed a deputy DPO. PV asked how much funding and how much salary levels were affecting recruitment? JH reported that it had been driven by both factors. It was noted that budget conversations were taking place at the moment and ARC members were keen that sufficient compliance officers were in place
- what planning was in place to prepare for the Senior Managers and Certification Regime (SMCR) for the insurance business? It was reported that the PO Insurance team had its own programme in place for SMCR as they were the Principal. CS would ask Amanda Bowe to touch on SMCR arrangements in her next report. It was reported that PO Limited liabilities for SMCR were being considered as part of the Legal Enterprise Optimisation work. It was noted that the FCA was very focussed on SMCR and group responsibilities in relation to this. **To do: CS**

5.3 **Information Security Policies Annual Review**

The ARC noted the papers and **APPROVED** the three updated Information Security policies on:

- Cyber and Information Security Policy
- Acceptable Use Policy
- Protecting Personal Data Policy.

6. Money Laundering Reporting Officer (MLRO) ANNUAL REPORT

6.1 Sally Smith joined the meeting and provided an overview of the key points from her MLRO Annual Report:

- there had been an increase in regulatory scrutiny from HMRC and we were receiving more information requests. Our HMRC relationship partner would be visiting the Chesterfield Office the following week to view our data and had recently visited 50 of our branches
- as more transaction data became available, more issues were identified resulting in more investigations activity. The data tool was currently sub-optimal and options were being considered

[1] In the middle of the Ofcom table.

POL00423454

- there had been three risk exceptions for products/ transactions over the period:
  - a minor risk exception in relation to the savings account journey on Horizon which had now been resolved
  - reliance on a paper mandate in the Deferred Checking Pilot for Banking Framework Services, for which we were seeking an automated solution
  - for the existing location exercise process.

6.2 A number of points were raised, including:

- whether we were set to achieve the June 2019 deadline for providing complete Fit & Proper data to HMRC? Timely responses from agents was challenging and significant work was underway to ensure data was received in time. Ultimately we had the option to revoke branches' ability to sell financial services products if they failed to respond. We were taking a targeted approach to get the branches with the highest volume of transactions and the new retail structure would assist this focus. Committee Members stressed the importance of enforcing the revocation sanction and it was reported that this had already been applied in some cases. Regular updates were requested on how on-track we were to meet the June HMRC deadline **SS**
- if registration costs doubled what impact would that have? It was reported that we had to make a decision in May 2019 about which branches would be registered to sell financial services products
- the PO Insurance MLRO report would be circulated to the Committee for information **SS/ VB**
- were we reporting in paragraph 36 of the report that we were going to be non-compliant throughout this year? It was reported that we were completing the 90 day regulatory transactions. What we had not been able to do was a holistic pattern analysis that would show particular pockets of issues but we were working to be able to introduce this reporting over the next few months
- MoneyGram compliance with Department of Justice (DoJ) Regulations. It was noted that we had obtained external legal advice on this issue and had met with MoneyGram's global head of fraud to gain a better understanding. The DoJ regulations related predominantly to transactions to and from the US. We would confirm that these responsibilities rested with MoneyGram and that they were now compliant with the DOJ regulations. **SS**

6.3 The ARC **REVIEWED** the report and the progress in addressing Bureau de Change controls and Fit & Proper requirements.

7. SECURITY STRATEGY

7.1 Rob Houghton and Mick Mitchell joined the meeting. RH reported that a more comprehensive Security strategy report was being provided to the Committee following the discussions at the Board meeting in November 2018. The next steps were to carry out a deep dive with Deloitte, following which it was suggested we provide quarterly reports to the ARC showing how we were performing against the metrics agreed. **RH/MM**

The strategy focussed on:

- the human element of weak passwords, susceptibility to phishing and so forth. There was an enhanced communications plan and a tool was being implemented to measure password strength. We were communicating with staff about these issues as well as testing password strength. We were making clear to people their personal exposure as well as their professional exposure where basic security requirements were not adhered to. JH would include regular reports on progress. This would be ongoing activity, not a programme of communications and training for a period of time
- third party suppliers and their security arrangements
- improving detection and incident responses
- mandatory training for new joiners as well as annual mandatory training for all staff, recognising that additional reinforcement was needed

POL00423454

- the recruitment of a Chief Information Security Officer (CISO) was in train and interviews were taking place the following week.

7.2 A number of points were raised, including:

- whether the risk appetite would be refined? It was reported that it would and that it would be helpful for the Board to understand the limits to what we could do
- whether we were looking at our third parties and requiring them to enforce security rules? It was reported that the ethical hack had demonstrated how important it was for us to monitor the security arrangements of our third party suppliers. We were setting up monthly meetings our top suppliers
- whether we would be monitoring sub-contracting by our suppliers? It was agreed that the whole supply chain would need to be monitored
- whether the CISO would have the "teeth" to be able to carry out their role effectively and whether reporting into the Group CIO was the right reporting line or if they should be reporting to someone externally? RH would give this further thought — To do: **RH**
- whether we should be benchmarking ourselves against the financial services sector as well as the retail sector? It was **AGREED** that we would benchmark ourselves against both sectors — To do: **RH/ MM**
- whether PO Insurance was covered by the Security Strategy? It was reported that they were as they bought our central services.

8. INTERNAL AUDIT REPORT

8.1 Johann Appel introduced the report and highlighted the key issues:

- the Internal Audit Team were now fully staffed and Deloitte had been on-boarded as Internal Audit co-partner. Five audits had been completed since October 2018 and eight were in flight. The relationship with Deloitte was developing well and their day-to-day management was good. We were meeting regularly with senior people at Deloitte
- a draft Internal Audit Plan for 2019-20 would be brought to the March ARC a more holistic approach had been taken to some of the audits we had been carrying out in Chesterfield and this was proving useful.

8.1 A number of points were raised, including:

- whether we had an agreed timeline for responding to Internal Audit reports and why it had taken so long for the Expenses Internal Audit report to be issued? AC reported that he had not been comfortable that enough work had been done to see whether we had any fraud risk before issuing the report, especially in relation to corporate credit cards. JA reported that the team had identified a significant number of exceptions to the policy that had needed to be investigated with receipts requested from credit card holders as well as testing a sample of employee expenses. It was noted that the team had looked at a large data set and had followed up the most significant exceptions. KM noted that he would rather that the Committee receive an initial findings report, setting out the further work which needed to be done and follow this up with a stage 2 investigation. Such issues and delays needed to be flagged to the Chair of ARC
- when had we had last reviewed the availability of corporate credit cards? It was reported that the recent review had led to the number of corporate credit cards being reduced from 96 to 35. We were in the process of on-boarding a new supplier which had better reporting capability. The expenses policy had been revised to align better with business requirements. The Selenity expenses system had been in place for a year and we had agreed to do some re-training for managers not only on checking the validity of expense claims but also ensuring that these were coded correctly. Committee Members noted that training was vital and individuals needed to be alerted when they were not adhering to the policy. There also had to be an onus on managers to check claims and the receipts. JA reported that spot checks would continue and a follow-up report would be undertaken in about six months.

POL00423454

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

9. AUDIT STRATEGY MEMORANDUM

9.1 Andrew Paynter introduced the Audit Strategy Memorandum. The meeting with EY had not taken place in October 2018 as planned originally but had now been held and a detailed file review undertaken.

PwC was hoping to be able to rely on the controls within Horizon. PO Limited was a complex business and significant systems change work had been taking place. PwC's approach reflected that this was a higher risk audit for them. PwC would being providing the same level of information it would for a listed company even though this was not a requirement for PO Limited.

EY had finished their final audit reports for PO Limited and these had been signed off; the only outstanding item was their formal resignation letter [*post-meeting note: EY's formal resignation letter was received on 13.02.2019*].

PwC's engagement letter had been agreed verbally. The Chair of ARC would be advised once all the appropriate paperwork had been signed off.

The significant risks for PwC were:

- Risk of Management override of control[2]
- Fraud in revenue recognition[3]
- Impairment of intangible assets subject to amortisation
- Impairment of fixed assets.

Postmaster litigation, would continue to be a focus and updates were received from Jane MacLeod.

The significant risks were prescribed by auditing standards and included data; ledgers with higher risk characteristics; any significant one-off transactions (e.g. the acquisition of Payzone Bill Payments); fraudulent revenue recognition.

Increased risk would be signalled by manual intervention requirements and particular attention would be given to those areas. IRS16, the new leasing accounting standard, had been issued. PO Limited had a high number of leases so this would have a material impact. Investment spending would also be a key focus.

The report set out the approach taken to financial processes in 2017/18 and how PwC would take this forward for 2018/19. PwC was seeking to bring the Horizon system into scope. PwC was finalising its work on the operation of the controls. The report set out PwC's proposed audit approach in 2019/20 as it transitioned from EY.

9.2 A number of comments were raised, including:

- that we had to make sure we were aware of any other work PwC was doing for PO Limited and that appropriate safeguards were in place
- that cash held in branch was a major risk for us. Andrew Paynter noted that reconciliations would be a focus for PwC. The move to a new system would not impact on this audit because it was retrospective. AC reported that we viewed cash as an elevated risk at the moment so this was a focus of activity for us. CS suggested that the audit tests proceeded as planned but that if a problem was identified this should be flagged and consideration given to re-categorising the risk
- why Successfactors remained out of scope for 2019/20? PwC reported that this would be an extensive piece of work but an issue they would continue to revisit. AC noted that we were starting to look at Successfactors' long-term strategic position, including considering whether

[2] Mandatory risk required by auditing standards, applicable to all audits.
[3] Mandatory risk required by auditing standards, applicable to all audits.

POL00423454

we were going to impair or depreciate. A deep dive into Successfactors was suggested, given the cost of the system and the limited functionality the system provided. **Exec**

10. COMMITTEE EVALUATION REPORT 2018

The recommendations of the Committee Evaluation Report were noted and the actions proposed were **APPROVED** as set out in the report.

The RCC would be testing risks to a greater extent with material risks being escalated to the ARC. The RCC minutes would also be provided to the ARC. There would be Non-Executive time scheduled with Internal Audit and the Finance Directors for the business areas would be given agenda slots periodically.

The meeting closed at 10.30 am.

....

Chairman **Date**

POL00423454

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
30 October 2018					
9. Business Continuity	An update on BCP to be provided.	**Tim Armit**	~~March 2019~~ May 2019	BCP now included on the agenda for the May ARC meeting.	Open
11. Insurance Policies	Review the risks covered by the suite of Insurance policies.	**Jenny Ellwood**	May 2019	Update to be given at the May ARC meeting.	Open
29 January 2019					
2. Updates from Subsidiaries					
2. (a)	Include the CMA's response to the super complaint as a potential strategic risk on the risk register.	**Jonathan Hill**	March 2019	We are checking that this risk appears on the Risk Registers for FS&T and PO Insurance.	Open
2. (b)	ARC to review the quality of sales of financial services products in the branch network in more depth.	**Jonathan Hill**	May 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting.	Open
4. Risk Report					
4. (a)	TC offered to put JE in touch with colleagues at BEIS who had a watching brief on potential insolvencies.	**Tom Cooper**	March 2019	**Done.** JE has meet with colleagues at BEIS.	To close
4. (b)	To provide an update on the EUM project	**Exec (Julie Thomas)**	March 2019	**Done.** The update is appended.	To close
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
6. (b)	To confirm responsibilities for complying with the Department of Justice Regulations rested with MoneyGram and that they were compliant with these Regulations.	**Sally Smith**	March 2019	A verbal update will be provided at the March ARC meeting.	Open
6. (c)	To circulate the PO Insurance MLRO Report.	**Sally Smith/ Veronica Branton**	March 2019	**Done.** The report is appended.	To close

POL00423454

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 22.02.19

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	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting.	Open

POL00423454

EUM Programme update

Author: Julie Thomas Programme Manager: Esther Harvey

Executive Summary

Context

The Enhanced User Management (EUM) Programme was first started in October 2016 in the FS & T area to ensure branches could continue to trade Financial Services products. A Smart ID would be issued to Horizon users only once they had passed vetting, and this was to be linked to their Success Factors learning records to prevent them transacting any product for which they were not fully trained. The solution would additionally cover all products where mandatary training was required to cover Post Offices regulatory obligations across a range of areas.

The original case expected all c.60,000 Horizon users to provide an individual email address and that they would use Success Factors to complete their training.

In August 2017, the programme had stalled due to operators and their assistants proving unwilling to supply individual email addresses or use Success Factors for their training. Historically, branches had been used to using Horizon for all training. Following a short review, a revised design and new business case was developed and approved by POL Board in January 2018.

This paper gives an update vs the revised case which, although represented a 12 month delay to roll-out and a £2.7m overspend to the original case, gave a solution which has succeeded in fully delivering the original desired outcome whilst minimising operational impact in our branches and for operators.

As the programme moves towards closure, a post implementation review has been instigated by the risk team to capture the key lessons learned during the entire duration of this programme.

Questions this paper addresses

1. What is the status and outlook?
2. What are the next steps?

Conclusion

1. The EUM programme remains on track for roll-out with 11,400 branches now live. 7,500 branches are now under training controls and demonstrating c.90% conformance with minimal reminder activity required. The rest of the network is

POL00423454

planned to enter full training controls by the end of February 2019 in time for the Insurance Distribution Directive becoming effective.

2. There are a number of remaining issues currently being worked through, including the 180 straggler branches who have yet to sign up and 2973 branches where full vetting is being pursued, but these issues are not expected to impact the programme's ability to deliver the full roll-out within budget.

Input Sought

The Committee was asked to note the current status of the EUM Programme.

POL00423454

The Report

What are we trying to achieve?

1. The EUM programme will enable Post Office to be confident that all Horizon users have been appropriately vetted, are up to date with mandatory training requirements, and we will be able to demonstrate this to our regulators across mainly Mails and Financial Services products.
2. In order to achieve this, a combination of EUM and Common Services Programme has collated detailed user data for every one of Post Office's c.60,000 front line colleagues. This data is stored in the SuccessFactors database, supported by SAP. The data holds verification of each user's vetting record and is accessed by Success Factors LMS and Forgerock to enable a Horizon user's Smart ID to govern the products they are able to transact on Horizon.
3. A significant barrier to overcome in the new design was the operational need for single operators to use 2 or more Horizon terminals so that they can process Drop and Go mail, serve Travel customers or prepare Mails despatches in between serving other customers. To achieve this, a 'suspend' function was introduced so that, although Horizon users can only use one terminal at a time, they don't need to complete the transaction in one basket to be able to start serving in the second.
4. Another requirement was to allow users to continue to use Horizon for their mandatory training, but to also give an option for them to use Success Factors since the long term goal will be to deliver all training via a purpose built LMS system. The design with SuccessFactors learning acting as the master for LMS and Horizon compliance data has allowed this flexibility.

What is the status and outlook?

Is the project on time?

5. The programme had been extended by 12 months, but is expected to complete roll-out to the entire fixed network by 28 February 2019, this is in line with the revised business case submitted in January 2018.
6. The main constraint on roll-out speed has been the Common Services Programme's ability to collect user data. Branches typically don't respond first time to requests for data and then the data provided is often incomplete. Contributory factors include absentee Postmasters where the Manager in charge does not wish to get involved in dealing with Assistant's personal data, and a large element of Postmasters who have simply not provided data because they did not wish to accept the controls this system introduces.
7. Close working with the NFSP has resulted in a greater acceptance for the change and this has been supported by a comprehensive communication plan which explains the benefits to operators and customers, in particular, Post Office's ability to win and retain new business as a result of this change.
8. There are c. 800 users in 180 branches yet to provide data to allow us to issue Smart IDs. These branches are currently being pursued in using an increasingly hardline

POL00423454

approach, starting with targeted communications, followed by a field team visit to assist the switch, and eventually the old Horizon ID will be disabled. This approach has been used so far on 700 branches with 95% success rate . Whilst this is incredibly resource hungry, the effort is not expected to have to be repeated as the JML process has been updated to ensure that all new joiners only have Smart IDs going forward.There are a further c.3700 users in 2973 branches who had never been vetted despite working in Post Offices for several years. These users are being chased continuously to provide data to allow us to complete the vetting checks. Any outstanding population will be reported at the end of the programme and, depending on numbers and the perceived risk they pose, a way forward will be proposed and a risk acceptance note prepared.

9. There is a current Change Request being progressed within Fujitsu which will prevent users logged on to two terminals from completing final balancing operations in one terminal while a second terminal is still in use. This has happened on 21 occasions over 6 months and is being closely managed by Fujitsu. As soon as an instance is reported, the branch is contacted to explain the balancing mis-match issues they may create and any issue is immediately corrected by the Transaction Correction team. A network wide communication was sent in early January. The change is expected to become effective from May / June 2019 and will not exceed the programme budget or require an extension of the programme team.

Is the project on budget?

10. The project is expected to complete with a £400k underspend vs the refreshed business case of £10.5m and this has been handed back as part of the recent forecasting process.

Is the project on track to deliver the planned benefits?

11. The key outcome of the project is to ensure POL is compliant with various regulations, mainly through ensuring 100% training conformance and locking users out of Horizon through training controls if they fail to complete training on time.
12. The latest training conformance rating was over 90% for SmartID users selling FS products. This performance has been achieved with minimal intervention by Branch Standards and the 7 FTEs in that team funded by EUM will come to an end at the end of March 19 as the programme closes.
13. Training controls are already in place for 7,500 users, and the rest of the network will be activated in February 2019, meaning all branches will be under training controls for future mandatory training modules from then on.

What are the implications?

Overall, how confident do you feel in the outlook?

14. EUM Programme is in its final stages of delivery with a high confidence level of effective completion.
15. The outstanding non-vetted population is now identified with a view to continuing to correct this anomaly. At the start of the programme, it was expected up to 10,000 users had not been vetted. This number was actually c.6000 and 3700 remain with clear follow-up actions in place.

POL00423454

Should we alter our plans or expectations?

16. N/A

What are the implications or lessons for any other part of the business?

17. The original EUM design had to be completely reviewed as a result of the early implementation issues. It has been documented and agreed that there was insufficient Retail or Network Operations input into the solution and this is the reason the sponsorship was moved to Julie Thomas who has extensive Network experience.
18. A Post Implementation Review has been started, led by Mark Baldock, Head of Risk. This review will be incorporated into programme closure documentation.

POL00423454

Financial Crime Risk Update

Author: Sally Smith Sponsor: Ian Holloway Meeting date: 20 September 2018

Executive Summary

Context

Post Office Limited provides second line financial crime services to POMS under the Master Services Agreement. This paper updates the Audit and Risk Committee on financial crime risks relating to Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF), and incorporates the Money Laundering Reporting Officer's (MLRO) annual report on compliance with The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 and The Terrorism Act 2000.

Questions this paper addresses

- What are the key AML and CTF risks within Post Office Managed Services Insurance products and are there any significant gaps or weaknesses in compliance with its regulatory obligations under the Money Laundering Regulations (MLRs)?
- Are the minimum control standards in the Post Office's Anti-Bribery and Corruption Policy being effectively applied?

Conclusion

1. Money laundering risks within the Post Office Management Services business are relatively low, and generally there are adequate controls in place to mitigate any AML risks that the business is exposed to.
2. Policies and procedures, monitoring and controls to mitigate Post Office Management Services exposure to financial crime are in place and communicated effectively to Third Parties.
3. Financial Crime Risk Assessments undertaken in May 2017 concluded that insurance products within Post Office Management Services remit were within the risk appetite set by the business. Although there have been no regulatory changes, and no issues or incidents reported or identified, these require annual re-assessment to ensure that this position remains.
4. We have not identified any instances indicative of Bribery or Corruption or failure to report and approve gifts and hospitality.

Recommendations for Action

5. Product managers must ensure that there is an up to date product information pack, which includes the treatment of PEPs and Sanctions checks to ensure that financial crime risk assessments are maintained.

POL00423454

6. POMS holds a detailed question set as a template for annual attestations for third parties to complete. At present, there are instances where the questions are not answered by third parties to evidence controls. POMS should ensure that the annual attestations are completed in their entirety by third party providers.

Input Sought

The Committee is asked to note the contents the MLRO report and endorse the recommendations.

POL00423454

Appendix A

The Annual Report of the Money Laundering Reporting Officer for the Post Office Managed Services Limited for the period 1st September 2017 – 30th August 2018

Table of Contents

A. Purpose and Scope of Report
B. Background
C. Governance Framework
D. Operation and Effectiveness of the Control Framework
  i. Senior management oversight
  ii. Staff awareness and training
  iii. Risk assessment, policies, controls and procedures
  iv. New products and services
  v. High risk products and services
  vi. Customer due diligence requirements
  vii. Reporting suspicious activity
  viii. Record keeping
E. Incidents and Investigations
F. External Threats/Landscape
  i. Business areas
  ii. The 5th Money Laundering Directive
  iii. The Criminal Finances Act 2017
  iv. The Policing and Crime Act 2017
  v. Joint Money Laundering Intelligence Taskforce
G. Conclusions and Recommendations
Annex A: Product and Service Risk Assessment Summary

A. Purpose and Scope of Report

1. The Money Laundering Regulations (MLRs) require that the Money Laundering Reporting Officer (MLRO) produces an annual report to appraise senior management on the effectiveness of key Anti-Money Laundering and Counter Terrorist Financing (AML/CTF) controls, and make appropriate recommendations for improvement in the management of risks and priorities, including resources where appropriate.

2. The MLRs and the 2017 National Risk Assessment clearly identify a requirement for organisations to adopt a risk-based approach to prevent money laundering and terrorist financing. Risk assessment must be documented and evidence the decisions that senior management have made in the context of the particular risks facing the business.

B. Background

POL00423454

3. Post Office Limited provides second line financial crime services, including AML/CTF oversight, to POMS under the Master Services Agreement.
4. General insurance products are not subject to the Money Laundering Regulations but firms operating within this sector remain subject to the Proceeds of Crime Act 2002 and are required by the Financial Conduct Authority to have systems and controls in place to prevent financial crime. Without these controls, firms are at risk of committing money-laundering offences. Therefore, most insurance businesses implement controls adopted by firms subject to the Money Laundering Regulations and AML rules.
5. There are a number of products and services that are sold or serviced through branches, the Internet and call centres which are provided on behalf of clients, or white labelled as Post Office. Whilst these products are regulated by the Financial Conduct Authority (FCA), the client or supplier is responsible for the regulatory activity. Post Office Management Services is required to meet its contractual obligations to them, but also to report any suspicious activity direct to the NCA, as required

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

6. The POMS Head of Risk and Compliance is responsible for oversight of compliance controls in place for POMS. The POMS Head of Risk and Compliance receives assistance from the MLRO of its appointed representative Post Office Ltd and the Financial Crime team to assess Post Office Management Services' exposure to financial crime.
7. Post Office Management Services has delegated regulatory training within POMS to Post Office Ltd. The training in place includes advising on how to proceed once an internal report and/or SAR has been made and the design and implementation of internal anti-money laundering systems and procedures.
8. Post Office Management Services' Appointed Representative, Post Office Limited, has a wider product and service provision for which it is regulated. Thus, Post Office Ltd is subject to further regulatory obligations. Following an interim appointment, the Head of Financial Crime, Sally Smith, took over as MLRO in September 2017. The MLRO is located in Finsbury Dials, Moorgate, London, where Post Office Group is situated.
9. The MLRO and Financial Crime Team report regularly on financial crime matters to the Post Office Risk & Compliance Committee (R&CC) and the Post Office Audit and Risk Committee (ARC).
10. The MLRO is the focal point of all AML/CTF activities and with the assistance of the Financial Crime team is responsible for assessing and assuring Post Office Limited's exposure to financial crime. This responsibility includes setting policies and standards relating to financial crime, assessing and assuring AML/CTF risks across Post Office, the provision of training and awareness within Post Office, the design and implementation of internal anti-money laundering systems and procedures, and advising on how to proceed once an internal report and/or Suspicious Activity

POL00423454

Report (SAR) has been made, submission of SARs to the National Crime Agency (NCA), liaising with third parties regarding investigations and ensuring information is appropriately disclosed to clients or third parties.

11. Where Post Office Management Insurance products are white labelled as Post Office and provided by a third party the responsibility for financial crime monitoring should be evidenced in the third party contract agreement and management information reported to Post Office Management Services on an ongoing basis.

12. Irrespective of whether Post Office Management Services owns the management and maintenance of financial crime risk controls or whether there is a reliance on third parties at a product or service operational level, Post Office Management Services should understand the extent of the financial crime risks posed across the business and the effectiveness and/or deficiencies of the mitigating controls. Both management and second line should ensure that the controls in place work as intended.

D. Operation and Effectiveness of Control Framework

i. Senior management oversight

13. See Section C above for summary of governance and oversight.

ii. Staff awareness and training

14. Provision of staff awareness and training is a key control for Post Office. All back office and customer facing staff are required to complete annual AML/CTF training:
    - For back office staff this must be completed within 30 days of joining and annually
    - For customer facing staff this must be completed before they have access to Horizon and annually

15. Annual training was rolled out in May 2018 to all back office and front office staff and agents.

16. Weekly monitoring of mandatory training completion levels for back office staff is provided to relevant HR Directors via Success Factors data for them to chase ,and where necessary, line managers follow through via performance management with individuals who have not completed training as required.

17. Directly Managed and Agency Branch Training is delivered via Horizon and completion is currently tracked by the Branch Standards Team. Smart ID is due to be rolled out to all branches by the beginning of 2019, and training controls are due to be implemented from September 2018 for those branches that have already migrated. These training controls will ensure that no customer facing staff will be able to transact regulated products on Horizon unless they have completed mandatory training.

18. An annual Training, Awareness and Communication plan is refreshed each year to aid the delivery of regular branch and business awareness communications on AML, Financial Crime and SAR reporting.

iii. Risk assessment, policies, controls and procedures

POL00423454

19. Post Office Managed Services have developed a comprehensive set of risk appetites for their business, which includes ensuring that it develops appropriate and balanced controls to mitigate its financial crime risk. In conjunction with POL these controls include measures to combat fraud, bribery and corruption, money laundering and controls to report effectively against sanctioned individuals. POMS has no appetite for public censure, fine or other significant regulatory sanction from any UK regulatory body arising from these financial crime risks.

20. Financial crime risk assessments are undertaken on all POMS products prior to launch and re-assessed annually, unless there is a product change or a material incident, in which case the risks are re-assessed at that time (see Annex A for a summary of the current assessments). The Financial Crime Team have been engaged to support risk assessment and risk mitigation for Project Nemesis (Motor and Household Insurance).

21. Policies relating to Financial Crime overall and AML/CTF specifically, were updated during 2017 and approved at the September 2017 Audit and Risk Committee. These clearly set out the minimum control standards required and who in the business is responsible for them, and are subject to annual review. Both first and second line management have responsibility to ensure that the controls in place work as intended.

22. The Financial Crime Team undertake assurance activity on the application across the business of the minimum control standards as set out in the policies, reporting any issues identified to the Post Office R&CC and ARC.

23. Additionally, the Financial Crime Committee, chaired by Jane MacLeod has been established to oversight the principle risk of Financial Crime across Post Office and is attended by the POMS Head of Risk and Compliance.

24. Claims handling poses a financial crime risk regarding fraudulent or false claims which require monitoring. POMS is not directly regulated for claims handling activities which are undertaken by other regulated intermediaries.

25. For Travel Insurance, claims handling is contractually outsourced by POMS to Collinson's and TIF, and for Life Insurance, claims handling is contractually outsourced by POMS to Royal London. All claims relating to sales prior to 1st January 2017 sit with the previous Life Insurance provider, Aviva. Regular reports are provided to POMS concerning claims handling by the respective intermediaries and POMS does not hold any direct regulatory responsibility for claims handling relating to Travel and Life Insurance. The business does remain exposed to reputational risk which is managed through the collation of management information and root cause analysis.

iv. Development of new products

26. There have been no new POMS products and services in the period under review. However, a Business Readiness Assurance approval process exists which involves multiple approval points that evaluate the confidence that the business has in accepting the change into its operational environment and ensures relevant AML/CTF risk assessment. The Financial Crime team ensure that all new or amended products and services have been through the financial crime risk assessment process prior to approval of Business Readiness.

v. High risk products and services

POL00423454

27. No POMS products are designated as high risk for money laundering.

vi. Customer due diligence (CDD)

28. POMS products are subject to basic CDD requirements and this includes checks for Politically Exposed Persons (PEPs) and Sanctions. For Travel Insurance, Sanctions and PEPs checking is undertaken by Post Office Management Services through Hexaware (due to migrate to Accenture during 2018/19). In respect of its other general insurance products, POMS relies on their third parties who undertake these customer checks, and should have in place processes to monitor that they are fulfilling their contractual obligations with regards to these activities.

vii. Reporting suspicious activity (SARs)

29. All staff are trained on identifying and reporting suspicious activity. SARs are reviewed and, where appropriate disclosed by the Fraud Analysis Team in Chesterfield under oversight by the Head of Financial Crime. The Financial Crime Team support more detailed investigations via liaison with relevant stakeholders where required. Where a third party is responsible for financial crime obligations, suspicious activity is identified and reported by them to the NCA, at which point Post Office Management Services should be notified by the third party in concerned.

30. To date there have been no SARs received relating to POMS products.

viii. Record keeping

31. All record keeping relating to AML/CTF is electronic (all paper SARs and paperwork are scanned and saved electronically) and filed within a restricted access AML drive under the control of the Head of Financial Crime.

32. All risk assessments and supporting documents are filed in the Financial Crime team drive, and a log is maintained to ensure annual review and sign-off.

E. Investigations and Incidents

33. There have been no investigations or incidents relating to POMS products during the last 12 moths.

F. External Threats/Landscape

i. Business areas

34. There have been no significant changes to the POMS regulatory landscape over the last 12 months. The National Risk Assessment required by the 2017 MLRs was published in October 2017, and did not identify high risk areas relating to POMS business.

35. The Financial Action Task Force review of the UK was undertaken during March and April 2018, but output is not expected before October 2018.

36. JMLSG guidance has been updated in the last year however there are no material impacts on POMS.

37. FCA in its annual report has said that one of its aims for the following year is to improve the UK's deference against money launders.

POL00423454

ii. Fifth Anti Money Laundering Directive

38. The Fifth Money Laundering Directive was announced on 30th November 2016 and its principle aims appear to be tackling the finance of terrorism. On 20th December 2017, EU ambassadors confirmed that agreement had been reached between the European Parliament and the Council regarding the latest amendments. These now need to be endorsed by the European Parliament and Council and they will then need to be transposed into national legislation within 18 months.

39. There are no significant impacts in respect of POMS products.

iii. Criminal Finances Act

40. The Act came into force in September 2017, and a working group was established by Legal with support from the Financial Crime team to ensure that a documented risk assessment was produced and measures put in place to establish a defence for Post Office. The primary risk relates to the criminal facilitation of criminal tax evasion by a Post Office 'associated person', although this is currently deemed to be low risk.

41. The working group have examined the reasonableness of procedures and controls relating to postmasters, contractors, employees and suppliers, and actions have been taken to address any areas of weakness.

iv. Sanctions and Anti-Money Laundering Bill

42. This bill was introduced on 18th October 2017, and it is designed to:
    - enable the UK to continue to implement United Nations (UN) sanctions regimes and to use sanctions to meet national security and foreign policy objectives post-Brexit; and
    - enable anti-money laundering and counter-terrorist financing measures to be kept up to date, helping to protect the security and prosperity of the UK and continue to align the UK with international standards

43. There are no significant impacts expected for POMS.

v. Joint Money Laundering Intelligence Taskforce (JMLIT)

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

45. The terrorist attacks in the UK in 2017 saw financial investigations being co-ordinated via the JMLIT members, and c.15 requests for information were responded to by members (including Post Office) in the hours after each event.

46. Prior to these attacks, the main terrorist finance red flags were to help identify funding activity for overseas terror groups, funding the outward or inward journeys of terrorist fighters, and the funding and activities of groups that preach or incite racial hatred. c.40% of terrorist financing is financed by low level criminality, basic fraud and robbery.

47. It is anticipated that going forward, security services will require the financial services industry to be able to do more to review 'pattern of life' activity, and focus more on domestic activity. In the 2017 attacks transactions were small, money was obtained and used quickly, often in cash or through other instruments like

POL00423454

prepaid cards and gift cards. The transactions are also consistent with normal activity – hiring vehicles, booking hotel rooms, buying kitchen equipment (knives) from supermarkets. The NCA have also advised that monitoring activity will be more about named individuals, and there is an expectation that there will need to be some regulatory or legislative changes to facilitate this.

G. Conclusions and Recommendations

48. Money laundering risks within the POMS business are relatively low, and generally there are adequate controls in place to mitigate any risks the business is exposed to.

49. With the size and complexity of the Post Office Network, one of the key AML/CTF controls for Post Office is robust training and awareness for all relevant staff. In 2017 there was an improvement in terms of corporate culture and individual responsibility towards regulatory training and monitoring completion, and the implementation of SmartID and training controls for Horizon users during 2018/19 will ensure that this is consistently applied across the business.

50. POMS have a responsibility to ensure that they support and promote effective training and awareness across product managers and sales teams.

51. The financial crime risk assessment methodology used for POMS products in May 2017 has been built into a replacement online product and service risk assessment tool for product managers to use for new products and services and this went live in April 2018.

52. All product managers are required to document a detailed product information pack, to inform this process, and POMS senior management should ensure that these are completed fully and in a timely manner to enable up to date product financial crime assessments to be maintained.

53. These product information packs should include the approach to PEPs and Sanctions checking for that product and cover the responsibilities of both POMs and third party suppliers in this regard.

54. Work has commenced with relevant product managers to produce product information packs for all existing products that were assessed in May 2017 to assist with the annual review process which is now due.

55. As highlighted in last year's report, POMS should ensure that the annual attestations are completed in their entirety by third party providers.

POL00423454

Annex A: Product and Service Risk Assessment

The last annual review of POMS products was completed in May 2017, a table of residual risk is below:

Service	Inherent Risk	Control Strength	Residual Risk
Travel Insurance	11.45	93.96%	0.69
Business Insurance	8.50	74.79%	2.14
Home Insurance/Over 50's Home Insurance	8.83	72.29%	2.45
Life Insurance/Over 50's Life Insurance/Free Parent Life Cover	9.00	87.29%	1.14
Car Insurance/Over 50's Car Insurance	8.83	74.79%	2.23
Motorcycle Insurance	8.83	74.79%	2.23
Van Insurance	8.83	74.79%	2.23
Pet Insurance	8.83	76.46%	2.08

The Financial Crime Team is at present assisting the POMS product managers to complete the groups Product Information Packs (PIP) for all POMs products. Once these have been received the above assessments will be updated.

The recurring theme in the assessments last year related to Post Office Group level risks, the majority of which have been mitigated during this year, for example, enhancing policies and SARs processes and ensuring there is a documented corporate structure. With this in mind we are expecting the above assessments to improve in these areas.

POL00423454

Appendix B

Anti-Bribery and Corruption Compliance

1. The ABC Policy was reviewed and updated in July 2018, and has been signed off by Post Office R&CC and ARC. The updated policy and a brief summary of the minor amendments is included in papers for POMS ARC for September 2018.
2. The new Gifts and Hospitality reporting tool was launched in August 2017, and reports are now provided to all Post Office GE members each quarter which summarise the reports received for their area and highlight any issues identified.
3. Since the launch of the new tool, there have been no gifts or hospitality reported for the Post Office Insurance employees. This is not inconsistent with the business sector, and all employees are subject to the same training, awareness and communications as Post Office employees.
4. Annual ABC training was delivered for completion on 21st August 2018, and as at the end of December completion rates across both Post Office and Post Office Insurance employees was c. 91%. Line Managers and HR Directors receive regular reports of those who have not completed training for escalation and intervention.
5. Regular communications are delivered via e-mail and One to relevant audiences to raise awareness of reporting requirements.

POL00423454

3.3

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 14 March 2019 at 11.30 am

Present:	Jane MacLeod (Chair) (JM)	Group Director Legal, Risk and Governance
	Catherine Hamilton (CH) (on behalf of Rob Houghton)	Business Performance and IT Transformation Director
	Mo Kang	Group HR Director
	Meredith Sharples (MS) (on behalf of Owen Woodley)	Director Telecoms
	Tom Moran (TM) (on behalf of Debbie Smith)	Network Development Director (items 4. – 12.)
In Attendance:	Veronica Branton (VB)	Head of Secretariat
	Jenny Ellwood (JE)	Risk Director
	Johann Appel (JA)	Head of Internal Audit
	Jonathan Hill (JH)	Compliance Director
	Colin Stuart (CS)	Finance Director – FS&T (item 4.)
	Russell Hancock (RH)	Supply Chain Director (item 5.)
	Nick Boden (NB)	Senior Product/ Travel Director (Item 6.)
	Sally Smith (SM)	MLRO & Head of Financial Crime (item 6.)
	Liz Robson (LR)	CIO – Retail (item 9.)
	Mick Mitchell (MM)	IT and Security Service Director (item 9.)
Apologies	Paula Vennells, Group Chief Executive, Alisdair Cameron, CFOO, Rob Houghton, Group CIO.	

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

Jane MacLeod opened the meeting and reminded attendees that the RCC role was developing and the Committee would be spending more time assessing and testing risk controls so that the ARC could focus its time on material risks having received assurance on how less material risks were being addressed.

2. Minutes and Action Lists

The minutes of the RCC meeting held 15 January 2019 were **APPROVED.** Progress on completion of actions as shown on the action log were **NOTED.**

Meredith Sharples reported that the ability to recruit to specialist digital roles had been considered further and was not considered to be a significant risk.

Jonathan Hill reported that an update on tax compliance had not been included in the March Compliance Report and it was suggested that a separate item on tax compliance be included on the May RCC agenda. **To do: VB**

3. Internal Audit

3.1 Internal Audit Report

Johann Appel reported that we were on track to complete 24 of the 26 scheduled internal audits (IA) for 2018/19. Two change assurance reviews would not be completed because there had been a delay in the programmes starting.

POL00423454

Support was sought to expedite the completion of the remaining 14 audits to avoid a high number of reports having to be presented to the May ARC. It was noted that the Contract management for IT IA was nearing completion with comments fed back by IT. The Cyber IA would not be ready for the March ARC papers but there would be an update note from Deloitte including a maturity assessment but not setting out all of the actions required. The maturity level had increased from phase one. We needed to understand clearly which items were high priority and which were material and to phase their implementation correctly. We also needed to understand any links between these actions and obtaining PCI compliance. The Cyber security paper for ARC would need to reflect the audit actions. The Network IA needed to be included with the March ARC papers. The IAs on Branch Hub and Agent Remuneration were almost complete.

A number of others IAs were in the field work stage and should be completed in time for the May ARC.

There were 5 overdue IA actions, all of which were less than 60 days late. These we not items of significant concern but would be escalated if they remained outstanding by the March ARC.

A number of points were raised:

- the PZBP Board would be meeting on 28 March 2019 and it would be helpful to update them on the PZBP IA and on the PZBP pen testing issue — **To do: VB**
- whether the Power BI app was used to produce automated network numbers? That was confirmed to be the case and it was fit for purpose from an internal audit perspective. JE reported that a review was underway on the Power BI app in relation to cyber security — **To do: JA and JE to discuss**
- why six IAs had been deferred to 2019/20? It was reported that ARC had approved a re-prioritisation plan in October 2018 to accommodate new IAs but the 6 deferred IAs remained on the plan to maintain their visibility.

3.2 Draft Internal Audit Plan 2019/20

JA reported the draft IA plan included input from the wider business and Bank of Ireland. It was noted that the areas of focus for change programmes should be regarded as a placeholder but we had a clear idea of our 5 governance reviews. We would start to do some deep dives into the governance programmes next year. The IA timings would depend on the timings for each of the projects. We knew when a new programme was coming on line and when the funding was approved and could then assess the risks. 28 audits were included on the plan and others were on the watch list as emerging risks. Good feedback had been received on the watch list items.

A number points were raised:

- whether GE Members had commented on the consolidated list set out in paragraph 11? It was confirmed that comments had been received from all GE members apart from Rob Houghton. Catherine Hamilton offered to provide comments from IT by the end of the week. It was reported that the timings proposed had been socialised. Timings had been fixed where this was required, otherwise timings were agreed nearer to the start date — **To do: CH**
- that the expenses IA should be jointly sponsored by Mo Kang and Al Cameron because it would cover the controls for payment of expenses — **To do: JA**
- whether contract management was a very broad focus for an IA? It was reported that this year's focus was on vendor management, focussing on revenue contracts with key material vendors
- that we should Include the proposed audit plans for PO Insurance in the ARC papers but note that these are subject to approval by the PO Insurance Board — **To do: JA**
- Appendix 2 of the report was discussed. It was agreed it was useful to understand how we were addressing different risks across a range of IAs but that the presentation could be clearer and a footnote should be added to explain that the numbers related to IAs. JA reported that for the May ARC the IA Team would be looking at mapping individual findings from IAs to the risks and thought was being given to how best do this and linking this to previous discussions about thematic findings.

POL00423454

4. Telco

4.1 FIN11 issue and Telecoms Controls

Colin Stuart provided an update on the additional financial controls introduced following from the FIN11 error. He explained that PO Landline and Broadband was provided through a group of suppliers with were brought together by Fujitsu as a service integrator. There were three financial streams, of which FIN11 related to accruals and payments. An error had been discovered in the accrual report. Fujitsu had corrected this and PwC had undertaken an independent review of the causes of error, the work required to resolve the issue, and the reconciliations. PwC had also looked at the FIN15 financial stream.

The error had occurred because there had been a mismatch between the reports run from the Fujitsu warehouse and the billing system. The over accrual had built up over time. The reconciliations and data had been corrected. PwC had found no other errors, excepting a small number of minor anomalies with a low value level.

A number of points were raised, including:

- whether CS and MS had confidence in the control findings and work done since the identification of the error and whether the business now worked better? It was reported that the overstatement had been 1% of revenue. Twice monthly financial interlock conversations were now taking place to test the trends we were seeing. We now had visibility of aged accruals[1] and that report would be moved into business as usual reporting. The fundamental problem was receiving data from a data warehouse which introduced an intermediation risk. That risk was being mitigated currently through a higher level of scrutiny and we also had greater understanding of the risk. Ideally we would get our data from the source and our current contract with Fujitsu ended in August 2020. We were buying tier 2 billing systems but there was a risk that the cost of getting data from the source, as was normal for tier 1 billing systems, would turn out to be prohibitive. In that circumstance we would carry our current intermediation risk into a new contract. The ability to supply data from source would be factored into the procurement process. The only action not fully completed from the PwC review was the analysis of aged accruals reporting but as noted this would be moving into BAU reporting. The IA report had found that balance sheet reconciliations had improved
- whether the improved controls in Telco had been extrapolated across the business? It was reported that there was more verification of finance reviews and standard reporting templates were being used. Quarterly business reviews took place with the CFOO and the central Finance Team as well as more testing and review at a business unit level. Grant Thornton was reviewing reliance on third party data. This review was due to be completed by year end
- whether we were looking at the risk of the security of the systems of third party suppliers? It was reported that we had a security framework and were testing this. It was suggested that it would be beneficial to apply this from a contract perspective. CH agreed to consider this further and apply some systems thinking by looking at a system end to end and how strong it was. **To do: CH**

4.2 Text Relay

Meredith Sharples reported that Ofcom had not yet given its decision on how it would respond to Post Office's non-compliance with text relay requirements over a four year period. We had expected the decision a few days ago. A Panel would take the decision and if it decided to investigate this decision would be published on their website. The working relationship with Ofcom had strengthened and we were also having monthly meetings with Fujitsu to discuss compliance issues.

It was reported that there remained uncertainty about the Telco regulatory horizon. Our approach was to be a fast follower of regulatory guidance. Vulnerable customers remained a risk for us, although this partly

[1] Which went down to customer levels.

POL00423454

depended on how vulnerable customers were defined[2]. As the business grew we became more visible and likely to attract scrutiny. Technical product change risk also existed by this was an industry problem rather than PO Limited specific.

5. Risk

5.1 Consolidated Risk Report

Jenny Ellwood reported that PCI compliance remained a key risk. Data discovery was still not complete and other work, such as reviewing the scripts sent out by ATOS, needed to be undertaken. The banks participating in the banking framework were monitoring our progress in obtaining PCI compliance carefully. Information Security work was on-track but we had detected a number of incidents, such as email address breaches and weaknesses discovered in the PZBP device through pen testing.

Updates were included in the report on the top 13 risks. Key person dependency risk was rated amber. JE had met with BEIS to see how they monitored third party financial stability. An important question for us was what we did with the data we collected.

Discussions on Risk appetite had been taking place, including the metrics we should use to assess whether we were within appetite.

Work had taken place to consider the suppliers on which we depended and what would happen if one of our multiples went out of business. This was reviewed on a monthly basis. It was **AGREED** that due diligence for multiples should be an agenda item for the RCC after next. The impact of litigation outcomes and the risks associated with this would be considered at the next RCC meeting. **To do: JE/ VB**

5.2 Brexit Update

JE provided an update on the latest Brexit situation and on PO Limited's contingency plans, which included communication plans, having additional people available in branch and looking at the practical impact of additional requirements such as customs forms. We were also monitoring where there would be any additional requirements or changed requirements for Data controllers and processors.

JE reported that she had met with the NFSP on 14 March 2019 and they were concerned about the potential impact of a hard border in Northern Ireland.

5.3 Back Office Transformation (BOT) – Legacy Risks

Russell Hancock provided an update on the BOT programme. He reported that there had been delays to the launch of the programme and moving to the new system. Timelines had become compressed and we knew that training staff to use the new system and then put this into practice would be challenging. Post launch, different systems were not interacting as we had expected them to and we had made some errors. We had since installed cash centre detectors, who had been early adopters of the system, to help identify and rectify system errors. Reconciliation errors had reduced to 27 last week. In addition, Transtrack had deployed their best staff on the project and users were better able to deal with system issues. We had identified super users and would maintain this group to assist other users.

A significant volume of work remained to be done. The wave 1 solution had been managing reconciliations via spreadsheets. We now had a data solution that was more robust. Planned order messaging had gone live two weeks ago and we were managing the risk of excess cash being in branches better through the Power BI app. The system still required manual interventions which was sub-optimal.

[2] E.g. a blanket inclusion of older customers.

POL00423454

We had expected a delay of 2 to 3 months before manual interventions could be removed; however, the Power BI solution may be sufficient as we resolve the reconciliation issues. A Steering Group was taking decisions on next steps.

JA reported that the Deloitte report on BOT had been sent to the CFOO the previous evening. The main conclusions were that the Transtrack report on the migration to CWC had been inadequate and that training had been insufficient. However, the reduction in the number of reconciliation errors had been so significant in the last week that we did not believe that an IA report would be required.

A number of points were raised, including:

- would we have made the "go live" decision if we had known what we know now? It was reported that the system was slower than we had hoped but that people not adapting to the new system had been the primary cause of errors. With hindsight more due diligence should have been done to ascertain that Transtrack had the required capability to move to CWC. We should also have included operators on the Steering Group to get better understanding of how the system needed to operate. A lessons learnt exercise would take place in due course
- whether we had been able to articulate what we needed the system to deliver in a granular enough fashion for a third party supplier? It was confirmed that we had but that the supplier's technology was built around cash centre operations and our requirements had been broader than this
- PO Limited was developing as a technology business. Due diligence and risk assessments were a prerequisite and we needed joined up and open challenge to enable us to ask the right questions. We needed to be cautious of reporting too optimistic a picture if there were issues to be addressed which could impact timing deliveries or the viability of the business.

6. Compliance

6.1 Compliance Report

Jonathan Hill reported that complaints for Telco on landline and fixed broadband were now below the average for the sector. We had a person dedicated to assessing the root cause of each complaint and the complaints handling system had improved significantly over the last couple of years. We were also aligning plans with our suppliers.

The regulator's response to the Competition and Markets Authorities' findings in relation to the super complaint was awaited and we did not know yet when their consultation would be issued.

The Payment Systems Regulator (PSR) had approached us last year and now wanted a further conversation on how our systems operated and how we supplied cash around the network. There was a drive to increase the regulation of PO Limited's cash supply across the network. However, we were not a payments system and the PSR would need Government consent to include PO Limited under their regulations. We were careful about describing what we did and did not want to be considered as a scheme.

6.2 Fit and Proper: Compliance with HMRC June 2019 Deadline

Nick Boden provided an overview of the Fit and Proper requirements and what PO Limited was trying to achieve through the Fit and Proper programme. HMRC required that we verify that Postmasters who carried out travel money transactions met the Fit and Proper requirements. The Fit and Proper programme was focussed on being able to meet the June HMRC deadline of providing data that would allow them to check our verifications. We were also considering options for annual returns and changes.

All agents and assistants should have been vetted at appointment but the HMRC regulations in relation to travel money transactions went beyond this and required knowledge of the products being sold, demonstrated through training undertaken. Where we could not provide evidence of compliance with

POL00423454

HMRC requirements we would "switch off" those branches[3] until we could provide the required information. It was noted that it was not easy to re-register branches. Branches with the highest revenue were being targeted but we were likely to have a tail of small turnover branches. By the next RCC we could show the impact of turning off some branches.

The programme had been running for over a year. A new programme manager had been appointed 6 weeks ago and had gained traction on programme delivery. Reporting out to the network had improved and we were receiving more robust reporting. At the end of February 2019, 1,800 full returns and 1,071 partial returns had been received. A backlog of 1,400 responses was being worked through. An integrated approach was being followed with people visiting branches and follow-up calls being made. The Programme also covered the multiple agencies. Verification of new branches would be part of the on boarding process.

A number of points were raised, including that:

- the Programme needed to build in the decision process for switching branches off, who would be taking these decisions and the operational impacts. This process needed to be in place by the end of March 2019. Nick Boden would produce a decision matrix and ask Julie Thomas and Amanda Jones to review this. The process needed to include the PO Limited senior contract for each of the multiples so they could speak with their counterpart where data returns had not been received **NB**
- there was concern about the potential for branches to be "switched off" from an agent and customer perspective as well as a revenue perspective. Sally Smith reported that she would be meeting with regulator in April 2019 and thought that if we could demonstrate robust figures and a clear programme for achieving full compliance HMRC might be prepared to extend the deadline.

7. Annual Legal Review

The paper was **NOTED**. Contract risks and framework risks continued to be flagged. Competition law risks were a focus in financial services and we needed to continue raising awareness about what information could and could not be shared. CH reported that setting up a community of practice for contract management was being discussed.

8. GDPR Update

The paper was **NOTED**. The GDPR programme was coming to an end. The Data Protection Officer (DPO) was a statutory role. We had asked our DPO to take a view on our level of compliance from a regulatory risk perspective and to assess whether we had a sustainable position. This assessment would be included as an item on the next RCC agenda. **To do: VB**

The GDPR work programme had been handed back from the GDPR team to Legal Team in October 2018. Since then a further 170 contracts had been identified.

9. Cyber Security Update

Mick Mitchell provided an update on the Cyber Security work programme, the business case for which was due to be approved today. The focus of the programme was reach, capability and putting in place a boiler plated quick response to incidents. Improving cultural awareness was a central plank of the work and this would be supported by the right tools and processes. Focus was also being given to the management of our third parties. A Chief Information Security Officer was being recruited and we now had a shortlist of candidates. £750k was being allotted to the first phase of the work with a total of £1.1m allocated in the change programme budget. We wanted to see the outputs of the Deloitte work in order to assess whether we should make any changes to our proposed approach but were prioritising work in accordance with an assessment of our key risks; this approach to prioritisation aligned with Deliotte's. The ARCHER work should underpin the Cyber Security work.

[3] A vetting failure led an individual not being able to process travel money transactions, a verification failure let to a branch not being able to process travel money transactions.

POL00423454

There had been three priority events since December 2018 and we were managing the data exposure risks. Breaches had been caused primarily by the use of weak passwords or using the same passwords.

A number of points were raised, including:

- what progress had been made with the cultural and educational programme? It was reported that communications had been issued and were continuing to be issued. There were going to be roadshows at key PO sites. Keeping the communications fresh and live was discussed. It was noted that communications would be ongoing. There was no finish point. Disruptive communications and approaches were being discussed at the next Information Security Committee and messaging was focussed on how security breaches impacted individuals
- whether we were deploying our best messaging resources? It was reported that we were working with the Communications Team. It was suggested that we should also be working with the Marketing Team and considering how we could use Digital Stars to support the messaging.

To do: MM/ JH

It was reported that there had been a recent instance where an individual had downloaded a significant amount of PO data. The data was mostly harmless but had included one sensitive item. The incident had been followed up with the individual but we needed to consider our policy on this issue further and the lessons learnt. It was noted that some of the Cyber Security investment was targeted at protecting our data.

PCI Compliance

Liz Robson provided an update on PCI Compliance. There were four work streams. The IT work stream was currently rated red. This was because while the pin pad devices to which we were applying point-to-point were supported for a reasonable period of time we had discovered that the current estate was only accredited until next Spring. We were seeking to align accreditation with the support timeline, working with Global Payments and INGENICO. It was reported that we had engaged DMW, a PCI specialist, to look at everything that we were going to need as we moved to the cloud. The IT team was working through the DMW report.

The PCI Compliance programme carried time and risk costs. Considerable attention was being focussed on this work but the scope of work had grown and we wanted to be sure that we had a full picture of the scope as soon as possible. It was unlikely that we would achieve full compliance by the end of the financial year because PCI compliance was binary and required all pin pad devices in every branch to be compliant. Work was already underway on point-to-point encryption of the pin pads. Communications had alerted partners to our non-compliance and progress briefings continued through relationship managers. Barclays had required a much higher level of information than other clients. We had produced a prioritised work plan and shared this under a Non-Disclosure Agreement (NDA) with Barclays. We were liaising closely with Global Payments.

Work streams were underway on remediation, PCI standards and on auditing. It was reported that PO Limited was now a member of the British Retail Consortium (BRC) and that as retailers bore the increasing cost of PCI compliance it could be a useful issue to raise with BRC.

PZBP

It was reported that IRM had been involved in pen testing and had been able to breach some PZBP devices. This testing was part of the PCI remediation work stream. An incident report had been raised and daily meetings were being held with PZBP to work through a priority order of activities. 201 transactions had been identified as potentials for fraudulent activity but we were analysing whether there had been any fraudulent activity in practice. We were looking at how we could secure these devices and working on a remediation plan. We did not believe there had been any breach at present and there was no impact on the PO Limited network. We were looking at moving PZBP transactions to the Security Operations Centre (SOC), the Legal team was exploring contractual remedy, and Andrew Goddard, the MD of PZBP, was considering compliance funding requirements for the longer term.

POL00423454

Committee Members asked whether we could have known about this problem and avoided it, whether we had assessed IT due diligence at the time of purchase and what the financial implications of a fraud could be. It was recognised that we needed to be cognisant of the reputational risks.

It was **AGREED** that a closing report on PZBP pen testing would be included on the agenda for the next RCC. **To do: VB**

10. Noting Papers

10.1 Procurement Update: Supplier Contracts out of governance

The paper was **NOTED** and it was flagged that a strategy for SSKs had now been approved by Rob Houghton, Group CIO, and a timetable agreed. Documents were with the Legal Team for final review and we should be able to issue the initial notices in the next week or so.

It was noted that some contracts, especially those for professional services, were not being procured in a compliant fashion. Non-compliance was going to be flagged in incident reporting on a weekly basis. People were not recognising contract renewal requirements early enough.

10.2 Horizon Scanning

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

The draft ARC agenda for 25 March 2019 was **NOTED** and discussed.

12. Any other Business

12.1 Treasury Policy

The Treasury Policy was **APPROVED** for submission to the ARC on 25 March 2019.

12.2 Contract management

Committee Members noted that improved capability was needed in contract management. Experience and capability levels were likely to be different in different parts of the business. It was an area for which a signature process might need to be developed and a theme that should be highlighted from the work being done by McKinsey.

12.3 Meeting dates

It was noted that the next scheduled RCC meeting was on 9 May 2019.

DRAFT

POL00423454

Risk Report

Author: Jenny Ellwood Sponsor: Jane MacLeod Meeting date: 25 March 2019

Executive Summary

Context

This paper provides an update on the key risks the Post Office is managing. The Central Risk team have also been reviewing the risk appetite statements and developing a plan on next steps.

Questions this paper addresses

- What are the key risks facing the business and what is being done to address these?
- What is the latest on risk exceptions and incidents?
- What are the emerging risks we face in both the short and medium term and what are we doing to address these?
- What is the latest position on Brexit and required next steps?
- What is the status of the Change Portfolio, its current top portfolio risks, delivery status and key delivery challenges?

Conclusion

- The paper reports 4 key risks: PCI, Information Security, Brexit, Change Workforce. It also provides an update on the Back Office Transformation Programme.
- Additionally following receipt of the judgement of the first trial work is under way to assess the impact, risk profile and the changes required.
- In terms of emerging risks and themes work is continuing to identify ways to improve the identification and management of any risks the change may bring to the existing businesses. We are also maintain a watching brief on the Loyalty Penalty Super Complaint and the risks this may create from a pricing and product perspective.
- An update on the performance of the Change Portfolio is provided of the Gold and Platinum programmes. The number of programmes reporting a red status has increased this reporting period. However, the view of the Central Portfolio team is that overall performance is good.
- The Change Excellence programme continues with the design and implementation of portfolio improvements and only one key risk is called out for information this month.

Input Sought

There are no decisions required at this time. The Committee is requested to note this paper.

POL00423454

The Report

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

1. There have been few changes to the heatmap status confirmed in January (see Page 4). However, it has been enhanced to show both this reporting period status and the previous one following a request from ARC. For red status, we have also incorporated a date on where we anticipate being back within appetite. Additionally, a principal risk on third parties has been incorporated and will be populated ahead of the next ARC. The judgment of the first trial is under review and the risk profile under both operational and legal and regulatory is likely to increase.

2. Appendix 2 shows the latest positon of the top PO Risks; this is held in the reading room for ease. There has been reduction in the Safety Compliance risk (Risk 13), which was formerly a red risk. This has been reduced to amber to reflect improvements in compliance. (Risk 9) regarding the risk of adverse outcome from the current Group Litigation needs to be reconsidered following receipt of the judgment of the first trial. It is currently scored as (5:2). The Key Person Dependency Risk (Risk 11) has been scored as Amber in the last three quarters. This could be removed from the Top PO risks.

3. As indicated by the heatmap the principal risk categories which are reported red and where focus is continuing are under Legal and Regulatory and Strategic (as per January's report).

4. Within Legal and Regulatory, PCI remains a key area of focus. The impact and probability score have remained the same at 16 (4:4). Although momentum is increasing, scope of our PCI environment is not yet fully defined. It must also be noted that the Data Discovery element has not completed and a new date of 31/3/19 has been suggested. DMW (external consultants) have been brought on board to perform a "root and branch" assessment of the IT work stream. The headline view is that our PCI scope has grown and this in turn will drive an increased cost and longer time to deliver. As such, programme delivery confidence is no more than 50%.

5. Additionally, IT Security's 19/20 Security Improvement Plan is in flight. Current activities to secure Post Office data, such as the implementation of DLP, Multifactor Authentication, 'Phishing' Campaigns and Password strength work streams are on track.

6. Within the Strategic category Brexit remains a red risk, although by the date of the committee we may be clearer on either an agreement on a deal, but more likely the terms of any extension approved by the EU. Work continues to mitigate the impact to the Post Office and a full update is shown in paragraphs 15-17.

7. Following a request from ARC in January 2019 to consider whether we have positioned the Financial Crime Risks correctly, the Central Risk Team alongside the Financial Crime team will be chairing Workshops with the

POL00423454

Products Managers. The results of this review will be presented back to RCC and to ARC in May 2019. A review on the way we manage and monitor key third parties, particularly around how we monitor their financial stability is underway, with Retail looking at a process for monitoring our key multiples. A meeting with UKGI took place to understand the process they follow.

What is the latest on risk exceptions and incidents?

8. Four risk exception requests have been approved since January RCC, all relating to IT change activity. The aggregate risk score ranges from low amber to green reflecting the low likelihood of impact on PO as risks are anticipated to be returned to within appetite by the latest April. Some have already been closed.

9. In two cases the request was to accept minor IT security vulnerabilities in order to prevent delay to the launch of a Branch Hub pilot. A third exception relates to system field changes made by MoneyGram which could not be fully tested prior to it going live. This was immediately tested in model office and no issues were identified. The fourth related to a potential data security vulnerabilities introduced by not performing pen-testing prior to the Azure data migration. The pen test was carried out and some vulnerabilities were identified and are now under review.

10. The Central Risk Team also worked with the business to ascertain whether a risk exception was needed to allow the use of temporary IDs for WH Smith staff required to work in newly franchised branches. WH Smith flagged they had been unable to get staff fully vetted due to delays in being unable to recruit. Activity is planned to raise awareness of the risk exceptions process and to encourage early engagement with the Central Risk Team.

11. The number of significant risk incidents reported over the last two months has remained at similar levels to the previous period. The two most common incidents reported are data breaches /potential breaches, and gas attacks on ATMs. An update on the data incidents is covered within the Compliance Paper.

What are the emerging risks we face in both the short and medium term and what are we doing to address these?

12. In terms of key emerging risk themes, work has commenced on identifying ways of improving how we identify and manage the risks which may arise from change within the existing PO business. Once this work is complete we will report back to RCC.

13. In terms of Insurance risk, an initial meeting has taken place with Locktons, we ran through the risk registers and themes for the Post Office and no high impact gaps were identified.

14. A watching brief remains with the Loyalty Penalty Super Complaint and the pricing and product proposition risks which this may create if the ruling is not in favour of Financial Services companies (the Compliance report provides the latest position on this).

POL00423454

Principal Risks	Trend / Risk Green Status Expected Date	Retail	Financial Services and Telecoms	Finance & Operations	Legal, Risk and Governance	IT	HR	COMM	Identity Services	ALL	Mar-'19 Comments
Operational	Jan-'19		↓			↓				n/a	**Red** – no high concerns reported in this area. The highest scoring operational risks in F&O reflect concerns about data accuracy and availability. The Data Analytics Excellence project is being re-planned and revised draft Business Case being produced y, Supply Chain capacity to meet future Banking Framework requirements and BCP (Risk 4). The Safety Compliance Top Risk has been reduced to Amber to reflect improvements in H&S training and compliance (Risk 13). **Key Amber points** – POLSAP migration has taken place. However, manual workarounds remain with cash centres and this continues to put pressure on teams. Work continues to resolve the issues.
	Mar-'19		↔			↑				n/a	
Information Security	Jan-'19									n/a	**Red** – Whilst Info Security is not called out red, Cyber Threat remains one of the highest top risks within IT and LRG (Risk 3). **Key Amber points** - A comprehensive Security Improvement Plan is in place and will continue throughout 19/20. It has been agreed that as Info Security covers all business areas the reporting of this will be amber across the board at this stage.
	Mar-'19									n/a	
Technology	Jan-'19									n/a	**Red** - no business area is currently reporting high concerns in this area. Retail continues to hold a key risk around the failure of IT infrastructure in branch, reflecting the importance of IT infrastructure in allowing branches to trade. Work continues with Retail and the BCP team to mitigate this risk. There have been no significant operational outages or issues since the last RCC report and service has remained stables overall so the risk level is unchanged. The Fujitsu campus failover remains one of the highest risks within IT. **Key Amber points** - POLSAP migration has taken place, all data is now live on the new systems and tested. Swindon Stock Services performed a successful failover test on the weekend of the 23rd February providing assurance of resilience.
	Mar-'19									n/a	
Third Party	Jan-'19	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	
	Mar-'19	New risk subcategory to be assessed in Mar/Apr 2019.									
Legal & Regulatory	Jan-'19	Re. PCI ↑	↓		Re. PCI ↑	Re. PCI ↑				n/a	**Red** - PCI remains a red area of focus within Legal & Regulatory category. Although momentum is increasing, scope of our PCI environment is not yet fully defined. It must also be noted that the Data Discovery element has not completed and a new date of 31/3/19 has been suggested. The red status also relates to a key risk we hold in relation to Cyber Threat (Risk 4) in LRG and concern over gaps and changes in agent data, where data provided to HRMC regarding Money Service Business is not sent on time or accurate. **Key Amber points** – FS&T Regulation Risk remains a concern (Risk 12). Intervention from Ofcom remains ongoing where meetings are underway weekly as part of the Mitigation Plan. Finance and Ops are reporting amber in relation to potential outcome of litigation in relation to the contract with agents. A watching brief remains with the Loyalty Penalty Super Complaint and the pricing and product proposition risks which this may create if the ruling is not in favour of Financial Services companies.
	Mar-'19	Re. PCI ↑	↑		Re. PCI ↑	Re. PCI ↑				n/a	
	Risk Green Status Expected Date	Jan-20			Jan-20	Jan-20					
Financial	Jan-'19									n/a	**Red** - no business area is currently reporting high concerns in this area. **Key Amber points** – In FS&T there is an increasing risk around inadequate financial controls. Detailed work plans are underway to ensure financial controls are in place and improved, targeted for end April 19. IT has missed the budget target but is delivering to 6+6. This position will not adversely effect POL overall.
	Mar-'19		↑							n/a	
Strategic	Jan-'19									Brexit	**Red** - 3 POL Top Risks (Retail) Proposition (Risk 2), (FS&T) Market Developments (Risk 6) and Brexit Implications (Risk 7). For the Retail Proposition, work continues on developing a new segmented proposition tailored to Agents and provide greater access to Post Office products and services. The Corporate & Market Developments risk remains Red. Board and GE signoff on strategy has been agreed and being implemented, projects and negotiations underway with BOI, RMG and development continues with digitisation for PO. Brexit remains a top risk across the organisation. Very little change in terms of understanding the possible outcome i.e.: a Deal, No Deal.
	Mar-'19									Brexit	
	Risk Green Status Expected Date	29-Mar-19	29-Mar-19							29-Mar-19	
People	Jan-'19		↓							n/a	**Red** - no business area is currently reporting high concerns in this area. **Key Amber points** - For the Digital Competency Risk (Risk 5), various streams of work are underway to support the Digital Workplace Programme (delivered by IT), this includes development of Talent Acquisition and Talent Development Programmes, introduction of Digital Stars - with ongoing workshops to upskill staff on the use of new platforms, engagement sessions with Business Units, regular communication of training programmes and e-learning in place.
	Mar-'19		↔							n/a	
Change	Jan-'19	↑		↑				n/a			The IT Controls Framework went live in January. Self-assessment requests are indicating that controls are operating effectively across the Change environment. A process of second line assurance of the IT Controls Framework will be implemented over the next quarter. Change portfolio tracking Amber. 8 portfolio risks defined. Top 3 are Portfolio performance, change workforce and business ownership. 8 'Platinum and Gold programme/projects are reporting Red RAGs (from a total of 41). These include Legal Entity Optimisation, Fit & Proper, Solar (aka Chameleon, HIH) and SF EUM Common Services. The current status reflects the overall position of the change portfolio considering scale and performance.
	Mar-'19	↔		↔				n/a			

↓ Improving ↑ Worsening ↔ Stable

POL00423454

What is the latest position on Brexit and required next steps?

15. Brexit 'No Deal' Contingency plans continue. An Operations Working Group is in place to ensure we have sufficient communications and training for branch colleagues. A call has also been made for management to be on standby for two days branch support during the 25th March and 5th April. Retail have identified the branches which may require more support.

16. Additionally, following further guidance from BEIS on Data, and a call Paula and Rob Houghton had with the MP Richard Harrington, we have expanded the list of third parties we need to write to. Contacting those that are data processors and who may be processing the data in an EU Country. So far no new issues have been identified.

17. Supply Chain have if required contingency plans they can deploy opening all depots on the weekends of 23rd and 30th March to provide additional services. Three reserve vehicles can also be in Portsmouth depot and teams can be deployed should assist Kent and East Sussex areas should traffic be heavy.

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

18. We have established a Change Risk Management Group (CRMG) who set the change risk strategy and policy. Its purpose is provide a proportionate, comprehensive and dynamic approach to the management of change risks across the Post Office.

19. CRMG is responsible for advising the Risk Director and the Strategic Portfolio Office Director on all aspects of Post Office change risk management and making appropriate recommendations to them on all significant matters relating to the Post Office's change risk strategy. It ensures all key change portfolio risks are ranked, responded to, reported on and reviewed. It ensures such risks have regard to the views of the Investment Committee and agrees those change portfolio risks (as well as any significant programme/project risks) which should be escalated to the RCC and ARC.

20. The overall status of the portfolio remains Amber. This is driven primarily by the fact that realised benefits for 2018/19 are forecast to be just outside tolerance (10.4% reduction) but looking to be recovered by the 3 year position. Investment for 2018-19 is amber. Work continues to improve the links between Project activities and deliverables and the benefits to be achieved.

21. 2019/20 portfolio prioritisation has been completed. It delivers the goals of the 3 year plan. An assessment against delivery constraints, which exist in our internal and external supply chain, is in progress. However, the judgement of the first trial, may need us to reconsider our priorities and focus.

22. Key risks are around increasing scope, mapping benefits to scope and the overall capability of the resource pool against the need of the portfolio (see

POL00423454

paragraph 26). This is reflected in an amber Resource risk. Changes are currently being implemented to mitigate these risks supported by a 'single source of truth' tool (Service Now) to ensure consistent quality data is enhanced. This has commenced incremental deployment.

23. We also launched, in February 2019, enhanced assurance activity including improved formal Health Checks on specific 'Gold' and 'Platinum programme/projects'. The latter has been piloted on Data Analytics and GDPR. A further seven Health checks have been identified between April–June 2019 subject to Investment Committee approving the final approach. These will be undertaken jointly by the Strategic Portfolio Office and the central Change Risk & Assurance team.

24. A summary of the current key 'Platinum and Gold' change programmes and their current reporting status is provided at Appendix 3. 8 projects are reporting Red RAG status. Key ones are:
    - Back Office Transformation (Delivery & Risk Red RAG): There is an issue with cash reconciliation, the root cause of which has not yet been resolved. The project will not now meet its planned completion date and there is further risk. Return to green dependent on root cause and resolution plan (see paragraph 27).
    - Data & Analytics (All themes Red RAG): Healthcheck identified concerns with the link between objectives and delivery approach and requested a re-baseline of the business case prior to further funding approval. Return to green dependent on acceptance of new business case (3/2019).
    - SF EUM Common Services (Cost, Delivery & Risk Red RAG): Project was requested to re-baseline prior to further funding approval. Return to green dependent on approval of revised budget, scope and timelines (3/2019).
    - Horizon Integration Hub (Solar) (Benefits Red RAG): There is a risk that the benefits originally stated in the business case will not be achieved. Return to green dependent on approval of revised business case (3/2019).
    - People Hub (Success factors) Phase 2 (Benefits Red RAG): Forecast benefits are not believed achievable so project will be brought to a controlled stop. Return to green dependent on approval of change request reflecting this (3/2019).

25. The CRMG consider there is one change related portfolio risk for the RCC/ARC to note (Change Workforce). This was initially referenced at the last RCC/ARC but the planned mitigations have been developed and made more specific.

Change Workforce

26. The delivery of the current short-term mitigations (by April 2019) will enable the scope of the issue to be assessed and the strategic solutions identified and begin to be implemented to bring the residual risk within appetite. This will have regard to the emerging Target Operating Model. Such mitigations include the collation of resource profiles for uploading onto Service Now, the rolling out of a Change Competency framework and the creation of specific

POL00423454

Communities of Practices for different change roles (such as project managers, Agile Scrum masters etc) to provide further professional support.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Change Workforce risk	The risk that incorrect resources (lacking the skills and capabilities) are assigned to change programmes. This would impact value and effective delivery. Workforce needs to be upskilled to obtain necessary skills and capabilities and costly recruitment will resolve short term gaps.	**12** **I/L: 4:3**	• Staff biographies are continuing to be collected to build full picture of skills and experience across the portfolio • The Strategic Portfolio Office Resourcing are formalising 30, 60, 90 working day check-ins with hiring managers to gather feedback on individual contractor performance • Deployment of Service Now-resource management tooling deployment planned for end of March. • Competency Framework -a key deliverable of Centre of Excellence –This will produce a baseline to allow the development of L+D plans and process standardisation to address skills. It is planned to revisit these in 6 mths	Complete By 3/2019 By 3/2019 By 4/2019	**3** **I/L: 3:1**

Programme updates - Back Office Transformation

27. At the time of go-live manual workarounds had been put in place to support 6 business processes and 1 system fix had been implemented. The business regarded the Supply Chain manual interventions as manageable but acknowledged that, at that point, the cash reconciliation process had not yet been undertaken.

28. Since then a number of issues are being proactively managed. These include:
    - Forecasting: the business have been using standard cash estimates for Branches which as expected led to increased cash holdings of around £50m across the network. An interim forecasting solution was planned for the beginning of March but has been slightly delayed. Branches are now reverting to pre-announced sterling values from standard estimates. This will prevent further increase in cash holdings. From a business risk perspective we agreed prior to going live that we could operate with standards for 3 months, and this level of cash in the network remains well under previous normal levels.
    - Reconciliations: We expected the Transtrack CWC to CFS financial reconciliation problem to deteriorate at go-live as volumes increased and new processes came on line. What was unexpected was an inability to fully reconcile the position between systems thereby explaining all variations. Although the project can now identify every missing transaction in Transtrack CWC further works is ongoing to identify all root causes. Over the coming 6-12 weeks the Transtrack development team are delivering fixes against a priority schedule every 2 weeks to resolve this problem.

POL00423454

Appendix 1. Post Office Principal Risks Definition

Principal Risks			Risk Definition
OPERATIONAL	Operational Risk	Process and Service Delivery	The risk of failed transaction processes or process management that are "externally facing" i.e. provide a service for external customers, including agents, clients.
		Product risk	Failure to successfully design, market, deliver, support and improve our product portfolio in a manner that meets customer needs and delivers desired customer outcomes, may lead to adverse financial and reputational impact.
		Payments (Demand / Regulatory)	The risk that Post Office is unable to manage effectively the payment process. Failure to comply with contract regulation, manage high volume of payments or record incorrect payments may result in a reputation damage and financial loss.
		Records management	Inadequate or insufficient processes and systems for creating, maintaining, retrieving and disposing of contractual, commercial, legal and intellectual property related documents and records, in line with legal and business policy requirements.
	Procure	Procure	The potential for failures in a procurement process resulting in loss, disruption, penalties or reputation damage. The management of the procurement channels is not optimal (reduced purchase options), and therefore could affect the continuity of the business and expose the business to incur high costs that could therefore reduce margins of profitability.
	Safety	Keep our people, customers & 3rd parties safe	The risk to health and safety of colleagues, contractors, customers and third parties (in the workplace, branches and also affected by business activities e.g. acquisition of a vehicle. Breach of Health and Safety regulations).
		Physically secure	Failure to ensure the physical safety of employees and agents in response to incidents such as theft, robbery, burglary, terrorism and site safety, could expose Post Office to significant costs for reimbursement for damages and remediation, operational disruption and reputational damage.
	BCP (excluding ITDR)	BCP (excluding ITDR)	The risk or instances of interruptions (including critical sites, critical and core infrastructure, suppliers and colleagues), as a consequence of internal or external events due to a lack of defined, tested and effective continuity plans and recovery strategies, which may lead to financial, operational and reputational damage.
	Reputation (Brand Protection)	Brand	The risk of losing the trusted brand image of Post Office that prevents the business from successfully operating in its chosen markets and/or achieving its North Star ambitions. The organisation may lose market share, key resources or its ability to compete because of the perception of its behaviour with customers, agents, suppliers and partners.
	Customer Risk	Customer Risk	The risk that business operations do not meet customer expectations due to a reduced focus on their satisfaction (e.g. vulnerable customers).
INFORMATION SECURITY	IT Security	IT Security	Inadequate procedures around the management of IT security resulting in cyber threat (denial of service, theft/unauthorised disclosure of valuable information) and insider threat (theft/unauthorised disclosure of valuable information, accidental disclosure, and illegal software use), and leading to financial loss, service disruption and reputational damage.
TECHNOLOGY	Business Interruption (ITDR)	Business Interruption (ITDR)	The risk or instances of interruptions to IT infrastructure and systems (including at IT suppliers) as a consequence of internal or external events and due to inadequate recovery strategies and/or continuity of systems and controls.
	Technology Ops	Technology Ops	Inappropriate, inadequate or unavailable technological infrastructure (e.g. HW, SW) to support current and future business needs in an efficient and effective way.
THIRD PARTY	Dependence on 3rd Parties and contract management	Dependence on 3rd Parties and contract management	The risk that Post Office is unable to effectively manage: - dependency on 3rd parties to deliver, support and improve services for which they have been contracted to the required time, cost or quality; and - its contracts, including failure to negotiate the favourable commercial terms and conditions in contracts, ensuring compliance with the terms and conditions, documenting and agreeing any changes or amendments that may arise during its implementation or execution, which may have an impact on financial and operational performance.
LEGAL & REGULATORY	Financial Crime	Managing losses and Fraud	The risk of acts that create financial loss, and/or are intended to defraud, misappropriate property or circumvent the law.
		Financial Crime	The risk of financial crime (money laundering, terrorist financing, bribery and corruption, fraud, etc.) resulting from inadequate or failed internal processes, people and systems, or from external events, leading to regulatory breaches and and/or reputational damage to the Post Office; and financial and commercial loss to the Post Office and its customers, colleagues and clients.
	Information Protection & Regulatory Compliance	Data Security	Inadequate procedures around the management of information and its security results in a breach of valuable information (customer, colleague, commercial and/or operational) leading to financial loss and reputational damage.
		Compliance with laws and regulations	The risk that Post Office faces exposure to losses, penalties and/or reputation damage when it fails to act in accordance with legal and regulatory obligations.
	Litigation	Litigation	The risk that legal action will be taken because of an individual's or organisation's actions, inaction, products, services or other events. Managers and employees, individually or in collusion, commit illegal acts, exposing the organisation, the management itself and the employees to their consequences.

POL00423454

Principal Risks			Risk Definition
	Record and pay taxes/VAT	Record and pay taxes/VAT	The risk that the administration of tax/VAT may be more costly - or otherwise more burdensome than foreseen. The risk may arise from existing tax/VAT laws and practice, or from changes in tax/VAT laws and practice.
	Governance	Governance	The risk that Post Office organisational infrastructure fails to provide robust oversight of decision making and the control mechanisms to ensure strategies and management instructions are implemented effectively.
	Conduct Risk	Conduct Risk	The risk of customer detriment or censure and/or a reduction in earnings/value, through financial or reputational loss, from inappropriate or poor customer treatment or business conduct.
FINANCIAL	**Financial Risk**	Reporting results, providing data accurately and effective internal controls	The risk that Post Office suffers reputational damage, loss of shareholder confidence and /or financial loss from the adoption of inappropriate accounting policies, ineffective controls over financial reporting, failure to manage the associated risks in changes to tax, law and failure to disclose accurate and timely information.
		Sufficient cash / headroom	The risk that Post Office is unable to maintain sufficient cash / headroom for the financial and operational needs of the business.
		Ensuring sustainable profit	The risk of not securing a sustainable and profitable growth (e.g. not focusing on the long-term performance) could reduce revenue and EBITDAS.
STRATEGIC	**Strategic Risk**	Competitiveness, Market and Customer Relevance	Failure to develop and implement an effective, coherent and consistent strategy: - aimed at establishing and maintaining a competitive advantage, in response to actions adopted by main competitors, disruptors or new operators; and - in response to changing markets (including demographic, technological and other external market events) and customers changing service needs and expectations.
		Strategic Risk	The risk that Post office does not have a Strategic Plan or deliver its North Star strategic priorities due to insufficient capability to execute it in line with plans or failure to adapt with agility to respond to changes in the external and internal environment.
PEOPLE	**Develop, Inspire and Grow**	Communicate, inspire and align	Inadequate, inappropriate or ineffective processes relating to recruitment, development, management, reward, engagement and well-being of Post Office employees could result in adverse financial, operational or reputational impact.
CHANGE	**Managing change**	Managing change	Inadequate and/or inappropriate capabilities, processes, organisation, data and culture to identify, prioritise, design, deliver and manage the portfolio of change activities resulting in delays, cost overruns, and non-realisation of benefits and in turn leading to the business not being able to operate the desire capabilities, processes and systems to support North Star ambitions.

Appendix 2. PO Top Risks

Please see the attached documents in PDF.

Appendix 3. Change Portfolio: Gold & Platinum programme/projects dashboard[1]

				RAG status				
Business Unit	**Project Name**	**Current Stage**	**Benefit Type**	**Cost**	**Benefits**	**Delivery**	**Risk**	**Overall**
LRG	General Data Protection Regulation	3 - Build	Compliance/ Regulatory	Green	Amber	Green	Green	Amber
LRG	Legal Entity Optimisation	2 - Design	Enabler	Amber	Green	Amber	Amber	Amber
LRG	Fit & Proper	3 - Build	Compliance/ Regulatory	Amber	Green	Amber	Red	Amber
Insurance	Nemesis (Home)	3 - Build	Income Generation	Green	Green	Green	Amber	Amber
Insurance	Morpheus (Pricing / CVM)	2 - Design	Income Generation	Green	Green	Green	Green	Green
F&O	Agent on-boarding	0-Initiate	Income Protection	Green	Green	Green	Green	Green
F&O	Branch Hub	3-Build	Cost Saving	Green	Green	Amber	Green	Amber
F&O	Back Office Transformation	4 - Test	Cost Saving	Amber	Amber	Red	Red	Amber

[1] Data taken from Change Monthly Executive Summary: February 2019 (P11)

POL00423454

				RAG status				
Business Unit	Project Name	Current Stage	Benefit Type	Cost	Benefits	Delivery	Risk	Overall
\F&O	Case Management	Handed to BAU	Cost Saving	Green	Green	Green	Green	Green
F&O	Cash Management	Handed to BAU	Cost Saving	Green	Amber	Amber	Amber	Amber
F&O	Future of Stock	2-Design	Cost Saving	Green	Green	Green	Green	Green
F&O	Data Analytics	1-Assess	Enabler	Red	Red	Red	Red	Red
F&O	Process & Contact Centre	2-Design	Cost Saving	Green	Green	Green	Green	Green
F&O	Safe Haven Exit	Handed to BAU	Cost Saving	Green	Green	Green	Green	Green
F&O	Source to Settle	2-Design	Cost Saving	Amber	Green	Green	Green	Green
F&O	SF EUM Common Services	5-Operate	Enabler	Red	Amber	Red	Red	Red
Retail	Enhanced User Management	5 - Operate	Compliance/ Regulatory	Green	Green	Amber	Amber	Amber
Retail	Mails Multi-Channel Customer Journeys	2 - Design	Income Protection	Amber	Amber	Amber	Red	Amber
Retail	Banking Framework 2	3 - Build	Income Generation	Green	Amber	Green	Green	Green
Retail	POCA Implementation	3 - Build	Income Protection	Amber	Amber	Amber	Amber	Amber
Retail	Cheque Imaging	5 – Operate	Income Protection	Green	Green	Amber	Amber	Amber
Retail	PCI Compliance	1 - Assess	Cost Avoidance	Amber	Green	Amber	Green	Amber
Retail	DMB	5 – Operate	Cost Saving	Green	Green	Green	Amber	Green
Retail	Crown Network Shape	5 – Operate	Cost Saving	Green	Green	Green	Amber	Green
Retail	Network Paddington	5 – Operate	Cost Saving	Green	Green	Green	Amber	Green
Retail	Network Transformation	5 – Operate	Cost Saving	Green	Green	Green	Green	Green
Retail	Network Development	5 – Operate	Income Protection	Green	Green	Green	Amber	Green
Retail	Horizon Integration Hub (Solar)	3 – Build	Enabler	Amber	Red	Green	Amber	Amber
Retail	SSK Simplification	5 – Operate	Enabler	Green	Green	Amber	Green	Amber
Retail	SSK Trial	5 - Operate	Income Generation	Green	Green	Amber	Amber	Green
Retail	SSK Procurement	2 – Design	Enabler	Green	Green	Green	Green	Green
Identity	Digital Identity	2 – Design	Income Generation	Amber	Amber	Amber	Red	Amber
HR	People Hub – Phase 2	3 – Build	Enabler	Green	Red	Amber	Amber	Red
FS&T	Travel App (Customer Hub)	5 – Operate	Income Generation	Green	Green	Green	Green	Green
FS&T	Home Phone & Broadband	3 – Build	Cost Avoidance	Amber	Green	Amber	Green	Green
IT	P2C Belfast Exit	3 – Build	Enabler	Amber	Amber	Amber	Amber	Amber
IT	Security Operations Centre	4 - Test	Compliance/Regulatory	Green	Amber	Green	Green	Amber
IT	Project Everest	3 - Build	Cost Saving	Green	Amber	Amber	Green	Amber

[1] Data taken from Change Monthly Executive Summary: February 2019 (P11)

POL00423454

Compliance Report

Author: Jonathan Hill Sponsor: Jane Macleod Meeting date: 25 March 2019

5.1

Executive Summary

Context

This paper provides an update on the regulatory and compliance matters in respect of Post Office's financial services and telecoms businesses, financial crime and information protection and assurance.

Questions this paper addresses

- What are the key compliance issues and what is the business doing to address these?
- What is the forward-looking regulatory agenda?
- What are the key policy updates in the period?

Status Update

Sector	Current Assessment	Previous Assessment	Comment/Action
Telecoms Compliance			Post Office is subject to an investigation by Ofcom into text relay. This is due to be completed by July 2019.
Information protection assurance			We are managing, with IT Security, three live data incidents but as yet, have had no evidence of data loss as a result of these. Where appropriate, the ICO has been informed
AML/CTF			All agents have now received a F&P letter and response rates/quality have improved, HMRC may also allow a short extension to the June deadline, but there is now a challenge from HMRC in respect of Officers in Charge. Still outstanding issues with the bureau de change transaction monitoring system but resourcing now in place to resolve
Whistleblowing			No material issues reported and communications and awareness actions from Internal Audit commenced
Anti-Bribery and Corruption			Minor non-conformances re Gifts & Hospitality reporting continue to be identified
Supply Chain Compliance			11 improvement needs from 4 audits in the 3 months to Feb. No material issues - satisfactory overall
Financial Services Compliance and Conduct Risk			Within appetite overall, however, 1. We are working with BoI on strategic product change initiatives that need careful conduct and reputational risk management in the coming months 2. Whilst mystery shopping results improved overall, there is a concerning hot spot for travel insurance sales and medical screening
Vulnerable Customers			Alternative format literature is still to be resolved for in branch materials-expected completion Mar 19

POL00423454

KEY:

	Material items of concern that require focussed remediation to ensure we stay within our risk appetite
	Some items of concern that could breach appetite if they crystallise or are not managed
	Within overall appetite

Input Sought

The Committee is requested to note this paper

POL00423454

Report

Key issues

Telecoms Compliance

Text Relay

1 In the last report it was noted that we planned to self-report the Text Relay issue to Ofcom. This was done on 7th January. We responded to Ofcom's questions on 21st February. On 14th March we were informed by Ofcom that it will be opening a formal investigation into our compliance with General Conditions related to Text Relay.

2 Ofcom has decided on this action due to the nature and length of time of the breach rather than its size, while acknowledging our cooperative approach to date, the new controls we have in place and our plans to refund customers. The notification has now been placed on the Ofcom Website, as a Consumer Enforcement Bulletin.

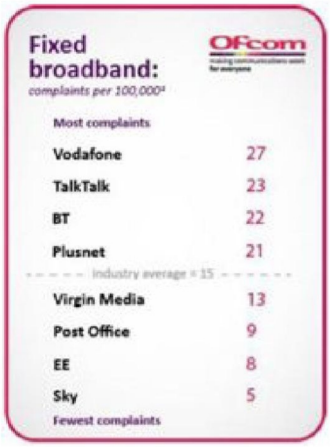
3 A formal investigation team has been established by Ofcom with an expectation to aim to reach a provisional view on the next steps in the case by July. We are establishing our own team to support the investigation (to include the Telecoms team, Compliance, Legal and Comms). Ofcom has stated it would be open in principle to a settlement on this case, and we are reviewing this approach.

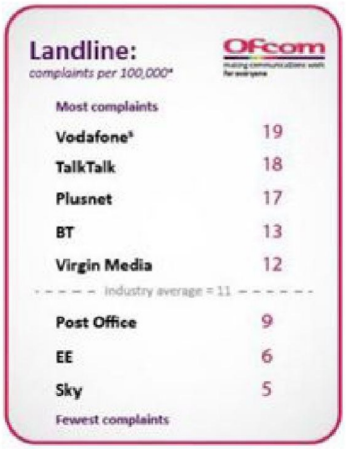
4 As advised to Ofcom we are in the process of compensating customers and will report back at the next RCC the outcome of how many customers we have been able to issue the refund to.

5 We expect to receive closer regulatory scrutiny in the coming year.

Complaints

6 Post Office appeared in Ofcom's broadband complaints table for the first time in January and were under the industry average. Post Office is also at our lowest level in fixed line, again under the industry average. Ofcom's complaints enforcement team is happy with our progress. Work still





POL00423454

continues on signposting complaints to ensure we are picking these up correctly.

7 Ofcom will publish its Comparing Service Quality Report at the end of April 2019. It is unclear yet whether we will appear in both broadband and fixed line sections. Work is underway on the S137A data request we received from Ofcom, which means we have to implement significant system changes in time to supply Ofcom with data for their report next year. Failure to implement the changes accurately or on time is subject to a fine.

Early Termination Charges ("ETCs")

8 Following Ofcom's scrutiny of ETCs (and fines applied to large telecoms firms) we received a letter in January 2019 reminding Post Office of its ETC transparency obligations on our website. We formally replied to Ofcom and met with its enforcement team, setting out the changes we are making to our web pages. Ofcom understood we were in the midst of changing the website and was satisfied with the new layout.

9 Also, informally Ofcom asked if we were changing our ETCs. We explained that we were reviewing our current ETC charging.

10 We do now expect to change our ETCs slightly in the coming months to ensure we are charging customers in line with the current sales channel mix and average tenure and to continue to ensure we are transparent and easy to understand. This had not been reviewed for a number of years and we do not have the historical business justification for the old charges, which may be challenged. The exposure to penalties from Ofcom has been assessed by our legal and business teams as low for two key reasons:

a. We have not been carrying out the sorts of charging practices (e.g., ignoring monthly discounts as part of ETC calculations) that caused EE and Virgin Media to get fined;

b. Changes in our ETCs will only increase or decrease by a small amount across our products and we have the same price across a customer's contract period.

11 Additionally, since early 2018, we have been trialling waiving ETCs if a customer challenges the charges in order to help improve customer satisfaction.

Information Protection & Assurance

Data Protection

12 Since December 2018, we have been the subject of 3 security incidents which have been actively managed. In addition, IT Security carried a pre-emptive phishing exercise across the organisation to raise awareness of the dangers of email phishing attacks. These are set out in detail in the Cyber Security Update paper. We have notified the ICO, including that we are working with the NCSC.

13 At the end of December 2018 we were alerted by the National Cyber Security Centre (NCSC) to 50 Post Office accounts being available through an Iranian state exploit of multiple companies. All 50 accounts had very weak

POL00423454

passwords and upon notification they were all promptly locked down and forced to use strong passwords.

14 At the end of February the NCSC alerted Post Office to inform that an extract of our Active Directory data is being offered for sale on the internet. The data for sale includes 10000 employee user names, office location and department, but not passwords. We have currently discovered no further breaches. Most of this data is publicly available. We continue to actively monitor this incident for any breaches.

15 Also at the end February Verizon Cyber Risk Program advised Post Office that a collection of 29 billion stolen users' credentials (usernames and passwords) had been published in the Dark Web in January. From these stolen users' credentials there were 40 that appeared to be from the Post Office. The source of the accounts were not obtained from Post Office systems. As a precaution those 40 accounts were disabled and their passwords were changed. A communication was sent to all Post Office employees to reiterate the importance of strong passwords and not to register for non-corporate services and applications.

16 In February 2019 we received a customer complaint that indicated we were using gov.verify customer data for Post Office marketing without consent. Investigations have shown that over 1 million customer records were incorrectly loaded into Brands, with a much smaller number having been marketed to. This was reported to the ICO but we were advised by the OICO that this was not a reportable incident. Nevertheless we have removed the customer records from Brands.

17 Bank of Ireland reported a breach in February 2019, which impacted up to 783 Post Office Savings customers who had been assigned recycled account number, which meant they could potentially see previous account holders E-Tac Certificates and/or E-Statements in their online account. This is under investigation. We are seeking clarity from BoI on how long this has been open, as well as customer communications to date. We are working with Post Office Savings team.

Compliance

18 We have successfully completed our external ISO27001 audit, conducted by Lloyds Register, with no major or minor non-conformities and have closed down the one finding raised during the last review in July 2018[1].

Financial Crime

Compliance with Money Laundering Regulations

19 Between 01.01.19-25.02.19, 55 new Bureau de Change non-conformance cases were identified. During the same period 74 open cases were resolved,

[1] The ISO27001: 2013 is an international standard for Information Security enabling Post Office to demonstrate ongoing commitment to information and cyber security. It is an operational requirement to be certified the UKVI service.

POL00423454

of which 34 related to customers who had purchased in excess of €15k in 90 days, which breached the regulatory limit.

20 In the 6 months following implementation of the new systems in June 2018, there were c.300 customers with linked transactions over Post Office's own lower £10k limit, of which c.80 breached the €15k regulatory limit. This demonstrates a very small percentage of the overall volume of Bureau de Change transactions, and is not yet at a level that would require investment in blocking transactions. Our HMRC supervisor is aware of this and we have demonstrated that we are taking appropriate action in each case.

Anti-Bribery and Corruption ("ABC") update

21 ABC training completion is at 98%. We continue to see some reporting non-conformances and have issued a specific communication about not accepting cash or gift cards and we have also provided detailed process flows on the Gifts & Hospitality intranet page.

Whistleblowing update

22 No material issues to report. As a result of the audit action in 2018, a Whistleblowing survey has been conducted via the Intranet to understand the level of awareness within the business.

Fit and Proper

23 A new Project Manager has been appointed to oversee the Fit & Proper project. We are now experiencing, with the support of Network Operations, improved response rates and are hopeful that there will be minimal outstanding branches in May 2019, when decisions about turning off Travel Money functionality will need to be taken.

24 We have engaged with HMRC to see if it is possible to extend the deadline from June 2019 to September, giving more time to close off outstanding records.

25 Following HMRC's branch audit in October 2018 HMRC has written to us, requiring us to identify where there are any cases of longer term postmaster absence/non-attendance, in which case Post Office is obliged to establish details of Officers in Charge (OIC) or Branch Managers and include this in our Agent Data submission. If we are unable to identify a suitable responsible person, we should cease providing over the counter currency exchange at those premises.

26 We are reviewing this new requirement with our legal team as an extension of the F&P requirements to OIC level would give rise to significant cost.

Regulatory updates

27 We continue to await information from HMRC of the anticipated fee increase, although we understand that proposals have been sent to HM Treasury. Budget provision has been made by the Travel Money team as a precaution.

28 The Office of Financial Sanctions Implementation (OFSI) has imposed the UK's first monetary penalty (£5K, having been reduce by 50%) for a breach of financial sanctions regulations on Raphaels Bank in respect of some of its Egyptian business. Whilst Post Office is not exposed to this type of risk, it demonstrates that OFSI are starting to apply penalties for non-conformance.

POL00423454

External threats

29 Between August '18 and February '19, 40 cheques totalling c£337K were deposited in branch into 8 different Post Office Current Accounts, Savings Accounts and Credit Cards and have been returned unpaid by the issuing banks. Due to processing delays this has enabled customers to transfer out funds before BoI was advised of the non-payment. The majority of accounts were successfully blocked by BoI but c£70K had already been paid. The Post Office Payments Team is liaising with Barclays (the cheque processor) to look at ways to prevent repetition and to have them refund BoI.

30 Further to the January 2019 MLRO report, we are awaiting the final legal opinion on Post Office's exposure to MLR requirements in relation to Banking Framework transactions. We believe that customer due diligence and transaction monitoring remain the responsibility of the banks but this needs to be confirmed.

Internal threats

31 Financial Crime risk assessments and re-assessments have been completed for 23 products and services, and a further 13 will be completed by April 2019. No major internal threats have been identified, and the outcomes are shared with the Risk Team to ensure that any risks are reflected within functional RACMs.

Supply Chain Compliance

32 Four audits were completed in the three months to February. 11 Improvement Needs identified with a combined audit score of 25, averaging just under 3 Improvement Needs and an audit score of just over 6, which mirrors the rolling average for all Supply Chain sites putting them in the Satisfactory category for both measures. No significant or recurring issues.

Financial Services

Travel Insurance mystery shops

33 Mystery shopping (7 out of 36) continues to identify counter colleagues not following the pre-existing medical conditions processes.

34 The risk is that customers could be given an inaccurate quote for travel insurance or potentially sold travel insurance they cannot claim on. However, we are unaware of any actual cases arising from customer feedback, attempted claims or complaints.

35 We are working with POI to improve communications on this issue and strengthening the sales process documentation to support an improvement. The new Insurance training module also went live in branches in February and should strengthen awareness.

Introductions of Loans on tablet via CRMs

36 This initiative launched in February and is the first time we have had an introductory sales process for loans in Post Office branches. FS Compliance will be overseeing that this process has embedded compliantly and gives customers a good experience.

Credit Card and Current Account changes

POL00423454

37 There are two significant changes (Credit Card and Current Account) that are being worked through with BoI. Both of these have the potential to raise concerns with customers and need to be handled sensitively.

38 As part of the Credit Card changes we expect to have another regulatory Principal and will need to agree working compliance arrangements with it and a multi Principal agreement with our other Principals, that does not conflict with existing T&C arrangements in branches and online.

Network management changes

39 We are working with the Network and Network Operations teams on the changes they are making to their branch management approach, including CRMs. The aim being to maintain appropriate oversight and conduct management but reduce the burden on the network teams

Vulnerable Customers

40 A series of 'One' communications is being issued to raise awareness and flag sources of external support.

41 The graduates are working on a branch check list initiative working with the Alzheimer's Society to help provide guidance to make Post Offices more dementia friendly.

42 A solution to in-branch alternative format literature for FS&T products should be implemented by the end of March.

43 We are working with an external third party to get an independent assessment on the capabilities of Post Office's vulnerability approach and how we can improve.

What is the general forward-looking regulatory agenda?

Citizens' Advice (CA) Super Complaint to Competition and Markets Authority (CMA) relating to the 'loyalty penalty'

44 CA raised concerns in November 2018 about long term customers paying more for goods and services, which it refers to as 'the loyalty penalty'. CA had identified five key markets where it has concerns about the loyalty penalty: broadband, mortgages, cash savings, insurance, and mobile.

45 Excluding mobile, all of these services are offered through Post Office channels. The CMA has strongly supported the CA complaint and is pursuing actions via the different regulators. To a large extent this is already supporting the direction of travel of the regulators Ofcom and FCA who are following a more interventionist agenda in their regulatory approach to the 'loyalty penalty' including price controls.

Telecoms/Broadband

46 Ofcom had already planned to introduce end of contract notifications and annual best tariff reminders for customers who are out of contract. At the same time of the CMA announcement in December, Ofcom also announced that it is reviewing the pricing differential. Ofcom has expressed concerns

POL00423454

about vulnerable customers who are out of contract and being charged high prices, with a particular focus on over 65s. We met with Ofcom in February as part of our on-going relationship and expressed concerns. Ofcom agreed that it shouldn't use such a broad brush to define vulnerability.

47 The telecoms team has reviewed its pricing strategy and analysed competitors' responses. The current decision is to maintain the current approach until the direction of travel from Ofcom becomes clearer.

Mortgages, Cash Savings & General Insurance

48 There have been no further developments from the regulator since the last report.

Other Telecoms Regulation

49 On 1st March the Broadband Speed Code of Practice came into force. This is voluntary and Post Office has not signed up to the Code, although we have already implemented key parts of it.

50 We expect the Automatic Compensation Code of Practice to be announced by Ofcom in the next few weeks. This again is voluntary and Post Office has not signed up. The challenge is that customers may expect us to be subject to the same rules and expect to receive compensation in certain situations. Conversations with Talk Talk to back off the cost of automatic compensation are still ongoing.

Access to Cash Review (Natalie Ceeney) and the Payment Systems Regulator

51 We (Martin Kearsley and JH) met with the PSR, at its request, to help them understand how the Banking Framework operates, how our bill payments business works and about our ATM business. At this stage it is simply for research but it is linked to Natalie Ceeney's Access to Cash Review, the final report of which was published 5th March 2019.

52 The review recommends increased regulation to preserve cash access, infrastructure and usage in the UK, calling out Post Office branches, cash in transit and bill payment capabilities as key to this.

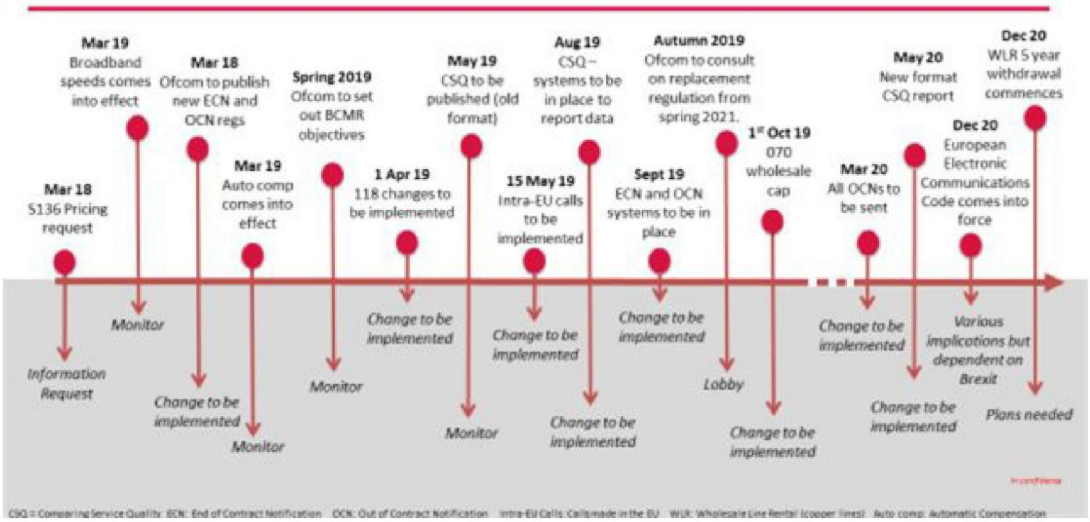
53 We have separately sought external advice as to our existing and potential future exposure to PSR regulation. Our initial review is that we are not subject currently but, with Government support, the PSR could extend its regulatory remit.

Jonathan Hill
Compliance Director
March 2019

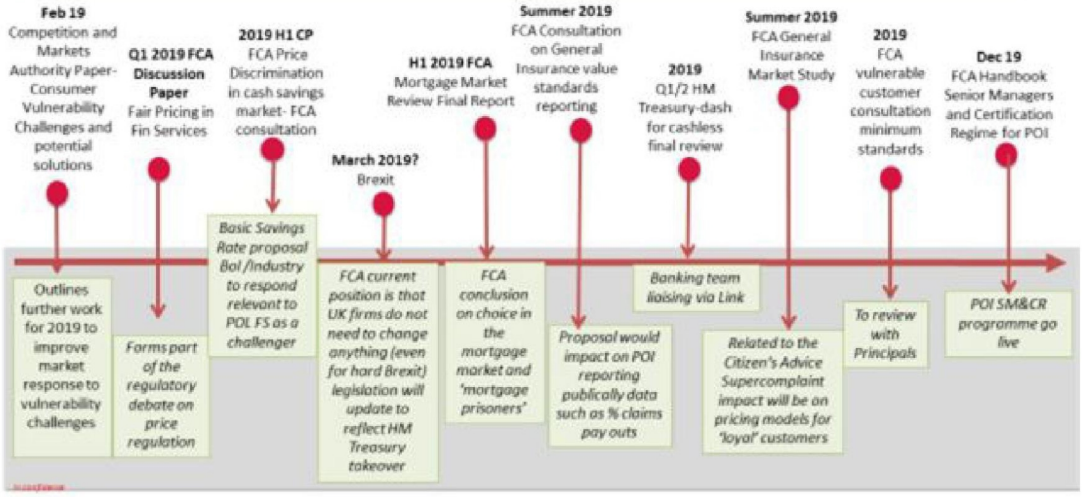
POL00423454

APPENDIX

Post Office Telecoms Regulatory Calendar



Post Office Financial Services Regulatory Calendar



POL00423454

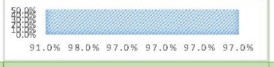
Tab 5.1 Compliance Report

5.1

	Key Risk Indicators				Performance								
	How we measure Compliance	Risk Rating	Risk tolerance	Measured in Jan-19	In each of the last months Aug-18	Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Key facts And Trends	Actions
TELCO	Slamming											
	A key general condition in telecoms is to ensure that customers are not miss sold telecoms products. We are awaiting a report from Fujitsu that details pre-five cancellations and reasons for this. This is a clear indication of how well we are selling products compliantly.		#REF!								TO BE REMOVED UNTIL SLAMMING REPORT IS GENERATED BY FUJITSU	
	Customer Satisfaction											
	Levels of customer satisfaction give an indication about how likely customers are to complain to the regulator and how the regulator will feel about our general performance as regulations are in place to protect customers. Bad compliance normally results in unhappy customers.		No less than 72%	#REF!	78%	79%	77%	77%	77%	#REF!	This reflects the journey we are now undertaking using the Customer First Programme.. It is also reflected in our lowest levels of Ofcom complaints too.	Continued focus on Customer First.
	Customer complaints sent to ADR											
	There are several metrics for complaints which we monitor. One area we measure is our Alternative Dispute Resolution stats. Complaints go to ADR when we fail to resolve the complaint in 8 weeks or cannot reach a resolution with the customer. This stat shows the amount of complaints going to ADR.		#REF!	#REF!	10	10	14	13	8	#REF!	We are currently working on improving our ability to pick up complaints early on. This is linked to improving our signposting score for ADR. As a result of this work, we may find the ADR complaints start to increase but these should then drop again as we rectify complaints early on in the process.	Focus on improved signposting to ADR. Ofcom are scrutinising Communication Providers complaince with picking up complaints.
	HP/BB % of colleagues trained											
	The number of colleagues who have completed the annual regulatory workbook and test		No less than 95%	#REF!	100%	90%	100%	100%	#REF!	100%	**The new learning test is due to go live on 22nd March. It is an annual test so metrics will change in the next report.**	Await new learning test in March to go live.
FINANCIAL SERVICES	Video Mystery Shops Rated RED BoI											
	The proportion of Agency CRM mystery shops for Savings rated red on a monthly basis for the last 6 months		No more than 20%	10%	5.6%	33.3%	0.0%	14.3%	16.0%	10.0%	A new in branch journey was introduced on the Tablet in October 2018, since then the VMS performance has improved greatly hitting 10% in January 2019.	Results continue to be reviewed and feedback provided to CRMs and ASPMS to help improvement.
	Video Mystery Shops Rated RED POMS											
	The proportion of Agency CRM mystery shops rated red for Life Insurance on a monthly basis for the last 6 months		No more than 20%	22%	40.0%	13.5%	20.0%	19.4%	22.2%	18.2%	Whilst the number of red rated shops has improved, this measure remains above tolerance. January shows 18.2%, this was partly due to a low number of shops completed.	The reasons for the fails remain the same, in particular where CRMs are failing to read health questions in full to customers.
	Counter Colleague Shops BOI											
	The proportion of Counter colleague mystery shops rated red in the previous 3 months		No more than 20%	6%	7.5%	8.9%	5.0%	5.0%	0.0%	7.1%	184 shops were completed in January, of these	One of the key areas measured is conformance to the provision of a Summary Box Leaflet to customers. This measure is showing an improving trend, however we are below the tolerance agreed with BOI (90%).
	Counter Colleague Shops POMS											
	The proportion of branch mystery shops for Over 50s and Travel Insurance rated red on a monthly basis.		No more than 20%	14%	6.7%	22.0%	19.0%	17.5%	0.0%	21.5%	296 shops were completed for Over 50s (115) and Travel Insurance (181) in January.	A deterioration in the number of reds was identified, in particular colleagues not following the correct sales process for customers with existing medical conditions for Travel Insurance.
	Mis Selling Upheld Complaints BoI											
	the number of upheld branch mis-selling complaints per 100 products sold		No more than 1%	0%	0.03%	0.00%	0.00%	0.00%	0.00%	0.00%	No misselling complaints have been identified	
	Customer Complaints POI											
	Total branch net sales vs branch distribution complaints received in the month		No more than 1%	0%	0.08%	0.00%	0.00%	0.00%	0.00%	0.00%	No branch distribution complaints were reported in January.	
	Over 50s life cancellations											
	The percentage of Over 50s sales cancelled within the 30 day cooling off period		No more than 10%	8%	1.50%	1.40%	1.70%	2.40%	2.40%	2.00%	Cancellation rates remain within tolerance	POL Compliance continues to monitor sales and cancellations using data supplied by POL
	Life Cancellations											
	The percentage of Life Insurance sales cancelled within the 30 day cooling off period		No more than 10%	7%	5.20%	7.60%	0.60%	12.00%	14.00%		Cancellation rates remain within tolerance	POL Compliance continues to monitor sales and cancellations using data supplied by POL
	Travel Ins Cancellations											
	The percentage of Travel Insurance sales cancelled within the 14 day cooling off period		No more than 2%	2%	1.50%	1.40%	1.70%	2.40%	2.40%	2.00%	172 policies were cancelled within the 14 day cooling off period .	Cancellation rates remain within tolerance
	Financial Services number of colleagues trained											
	The number of colleagues who have completed the annual Financial Services regulatory workbook and test.		No less than 95%	95%	1.50%	1.40%	1.70%	2.40%	2.40%	2.00%	Financial Services workbook was completed during the period 7/1/19 - 30/1/19. 95% of colleagues have completed the training.	
	Insurance workbook number of colleagues trained											
	The number of colleagues who have completed the annual Insuranceregulatory workbook and test.		No less than 95%	95%	Will get results from end of March-new module						Insurances workbook was completed during the period	
IPA	DP Incidents											
	Number of DP incidents		no more than 3	3	1	3	1	1	#REF!	4	These are four significant data issues, 3 being worked on with IT Security and one with Identity	
	Supplier Management											
	The number of overdue actions from Tower Suppliers		no more than 1	7 (TBC)	This is is a new metric and thus not RAG rated this month. We are working with the Tower suppliers to close actions quickly.							

POL00423454

Tab 5.1 Compliance Report

	IS & DP % of colleagues trained						
	The number of colleagues who have completed the annual regulatory workbook and test. Weighted average between support and branch figures		No less than 95%	97%			
FINANCIAL CRIME	Bureau - customer transaction limit breaches						
	This is the number of customers that have breached the £10k in 90 day limit for in branch Bureau de Change and have been identified from transaction monitoring.		Witihn appetite firm metric tbd	24		This is a key measure as Post Office is directly regulated by HMRC and has previously received fines for poor controls.	Given the immaturity of the new data monitoring, a risk tolerance will be set once the level of impact from breaches has been understood
	Supply Chain Audit Issues						
	Measure of effectiveness of supply chain compliance with industry regulation. ACS and ISO accreditation are required to maintain our cash supply and retain our NCS status		Seriously Adverse (>24 score)	0%		Measure of effectiveness of supply chain compliance with industry regulation. ACS and ISO accreditation are required to maintain our cash supply and retain our NCS status	
	ABC % of colleagues trained						
	The number of colleagues who have completed the annual regulatory workbook		No less than 95%	98%			
	AML % of colleagues trained						
	The number of colleagues who have completed the annual regulatory workbook and test.		No less than 95%	98%			

5.1

POL00423454

The Fin11 issue and Telecoms Controls

Author: Colin Stuart Meeting date: 25th March 2019

Executive Summary

Context

Post Office's Telecoms business provides broadband and landline services to customers through a selection of providers, managed by Fujitsu as the overall service integrator.

Post Office uses reports generated by Fujitsu (known as Fin02; Fin11; and Fin15) to account for revenue. In May 2018 Post Office identified an error in the Fin11 report which had the impact of overstating income by £5.2m in 2017/18.

Fujitsu corrected and restated Fin11 and PwC conducted an independent review which established the cause of the error, reviewed the correctional work, conducted reconciliations and reviewed the business logic behind the generation of the Fin11 and Fin15 reports. A satisfactory internal review of the Fin02 report had previously been carried out.

This paper sets out the causes of the Fin11 issue, its resolution, the conclusions drawn, and the actions taken to strengthen controls in Telecoms and in the wider Post Office.

Questions addressed in this report

1. What was the Telecoms Fin11 issue and how did it arise?
2. How was the Fin11 issue resolved, what were the conclusions and what are the recommended actions to prevent a recurrence?
3. How well does the improved Telecoms control environment manage the risks?
4. What are the potential wider control issues and how have these been addressed?

Conclusion

The Fin11 issue arose from a mismatch between the billing system and the Fujitsu data warehouse which resulted in records being incorrectly treated as live in the Fin11 report, but correctly treated as on-hold by the billing system.

The issue was resolved by Fujitsu correcting the Fin11 report and refreshing the data warehouse from the billing system. An external independent review by PwC validated and reconciled the Fin11 and Fin15 reports, confirmed the business logic behind them and verified that there were no other significant errors. A list of actions was prepared to address the control environment in Telecoms and the wider business.

Good progress has been made on the actions, with the majority implemented and the remainder underway. The improved Telecoms control environment manages the risks, but the Fujitsu data management and reporting structures mean that risks remain and these require high levels of verification and review type controls in mitigation. In September 2018 this improved control environment identified a smaller (£0.4m) issue with Fin11 relating to old New Call records. The arrangement with Fujitsu is being retendered in 2020 and clear requirements for data management, controls and reporting will be included as part of the specification for that.

Input sought

The ARC is asked to note the contents of this report, questioning and challenging as appropriate.

POL00423454

The Report

1. What was the Telecoms Fin11 issue and how did it arise?

1.1. Post Office's Telecoms business provides broadband and landline services to customers via a selection of technology and service providers, managed by Fujitsu who act as the overall system integrator to provide a packed service. The business has revenues of c£155m and direct contribution of c£30m

1.2. Fujitsu generates three reports which Post Office uses to account for revenue:

- Fin02 - which details customer balances
- Fin11 - which calculates deferred and accrued revenue
- Fin15 – which provides summaries of invoiced net value

1.3. In May 2018, Post Office reviews identified an error in the generation of the Fin11 report. The issue was caused by the billing system (operated by MDS) correctly marking records relating to the Line Rental Saver promotion as on-hold, but that status not being recorded in the Fujitsu data warehouse. The Fin11 report uses that data warehouse as its source of information. As a result, Fin11 incorrectly accrued income in respect of c117,000 records over a 15 month period, resulting in an overstatement of revenue in Post Office's books totalling £5.2m.

2. How was the Fin11 issue resolved, what are the conclusions and what are the recommendations to prevent a recurrence?

2.1. The issue was resolved by Fujitsu correcting the Fin11 report and refreshing the data warehouse from the MDS billing system.

2.2. Independent external reviews by PwC of Fin11 and Fin15 were completed in July (Fin11) and August 2018 (Fin15). These validated and reconciled the Fin11 and Fin15 reports, confirmed the business logic behind them and verified that there were no other significant errors.

2.3. The PwC work also considered why the error was not discovered earlier. The conclusions were:

- Reliance was placed on the incorrect assumption that the Fin11 report produced by Fujitsu was an accurate reflection of the data in the underlying billing system.
- The level of rigour and scepticism applied to understanding the reasons for the increase in the Line Rental revenue accrual was insufficient given the trend in the balance and the size of the size of the error.
- There was a lack of clarity/understanding of the contract with Fujitsu with regard to the roles and responsibilities (at both Post Office and Fujitsu) for ensuring the accuracy of data held within Fujitsu's data warehouse and how the billing system data was used to populate the data warehouse.
- Documentation of the monthly balance sheet review did not have sufficient factual support to validate the comments made. Process documentation to ensure the robust and consistent application of the review was not in place.

2.4. PwC prepared a list of Telco specific recommendations to address the weakness in the control environment:

- *Ageing assessment*: Identification and scrutiny of the Line Rental accrued revenue balance would have been facilitated by an effective aging analysis. It was recommended that Post Office work with Fujitsu to create a report.

POL00423454

- *Independent checks*: Post Office should further develop the process of periodic review of the information within the Fin11 versus other trends and balances.
- *Impact on other reports*: As PwC's work focused primarily on the level of accrued revenue, they also recommended that any other potentially misleading statements within the regular monthly reporting commentary should be identified and considered.
- *Supplementary Reporting*: PwC noted that they were made aware of additional "drill down" reports that are available but those reports did not appear to be in regular use. The additional level of detail contained therein may have assisted in the more timely discovery of the issue.
- *Risk Assessment*: Post Office should develop formal guidance to support the risk assessment that takes place as part of the monthly balance sheet review. This would assist in a more rigorous and consistent approach.
- *Data Retention*: Post Office should insist on a level of data retention from its suppliers to ensure that any future errors are identified and preserved to allow any re-performance where necessary.
- *Data integrity*: POL should consider the contractual responsibility for confirming the accuracy of the data within the Fujitsu data warehouse.

  The actions developed to address these recommendations and their current status are set out in Appendix 1.

2.5. Good progress has been made in implementing PwC's recommendations. The key outstanding point is the aged analysis reporting from Fujitsu which has taken time in the scoping and definition phases, and in finding a build slot. A draft report is available, has successfully passed testing and is moving into production, with acceptance anticipated in March 2019 for use at the 2018/19 year end.

3. How well does the improved Telecoms control environment manage the risks?

3.1. The improved control environment and regular formal interlock between Telecoms and Finance have increased our ability to manage the risks of the Telecoms business.

3.2. In addition, the general level of scrutiny applied by the Telecoms and Finance team has increased significantly, with detailed joint review of weekly data. This has identified small items for correction/follow-up with Fujitsu that might previously have grown unnoticed.

3.3. However, there are inherent risks with the interface between the Fujitsu Data Warehouse (that is used as source for our financial reporting) and the MDS billing systems. The ideal would be for reports to be directly derived from and automatically reconciled to the billing system. However, the Fujitsu contract is being re-tendered in 2020 and so large scale changes would be expensive and potentially short term. We will ensure that our requirements for robust reporting, data integrity and a strong control environment are incorporated in to the re-tender documentation. In the meantime we will continue to mitigate the risks using the higher levels of scrutiny described.

3.4. In September 2018 the greater scrutiny and stronger controls between Post Office and Fujitsu highlighted a data issue within the Fujitsu data warehouse. The impact was relatively small at £0.35m and occurred in relation to the transfer of customers in the New Call acquisition in 2017:

POL00423454

- In between the data extract and the actual transfer date around 1,000 New Call customers indicated that they did not want to transfer.
- Steps were taken at the time to ensure that the accounts were never live on the network and they were marked as closed on the MDS billing system.
- However, the corresponding records in the Fujitsu data warehouse were not removed and Fin11 accrued revenue monthly in error.
- The erroneous records have since been removed from the Fujitsu Data warehouse.
- In their review of Fin11, PwC noted the New Call customer records in the data warehouse. They estimated their financial impact to be less than £1k and noted their pending deletion. As a result PwC did not perform or recommend any more work.

3.5. We have also identified that the model currently used for budgeting and forecasting has become complicated and unwieldy, making it prone to manual error. We propose to rebuild this in Q1 and are in the process of bringing in a specialist contractor to assist.

4. What are the potential wider control issues and how have these been addressed?

4.1. The Fin11 issue highlighted some areas of potential improvement across the wider business:

- Overreliance by Post Office on third party data for revenue recognition
- Inadequacy of processes and controls in place at third parties
- Lack of understanding by Post Office business owners over processes driving revenue recognition
- Lack of existence and robustness of controls and reviews around third party data

4.2. Previously, the focus in the Post Office control environment was on granularity of controls – aiming to mitigate all risks, big and small, through detailed controls.

4.3. Prompted by the Fin11 work, changes have been made over the past 6 months which involved creating a more rounded control environment. This has included establishing an appropriate level of detective and preventative controls for key risks:

- *Good quality balance sheet reconciliations* – the old "probity" process was inadequate. The new process focuses on the user of the reconciliations i.e. what information would someone require to identify an issue in the balance. Training has been given across the business and new reconciliation templates have been implemented.
- *Supportable analysis* - balance sheet reviews should be less discursive, instead focussing on agreeing items back to support and performing analytical and ageing reviews. These are now performed routinely, with quarterly deep dives.
- *Appropriate challenge of management* – regular formal meetings with management to understand and challenge trading, balance sheet trends and balances in the context of business logic and performance. These are in place.
- *Review of detailed controls* – detailed controls have been reviewed for naivety; irrelevant controls have been removed; controls have been re-worked to ensure a risk focused approach; and a detailed review of processes linked to

POL00423454

Back Office Transformation has been carried out. This has resulted in numerous changes to controls. An ongoing cycle of deep dive reviews is planned.

- *Assurance where reliance is placed on third parties* – an assurance exercise is underway in areas where Post Office relies on third parties for revenue recognition. A review of revenue streams identified 13 third party suppliers for further work. Of these, 7 were deemed significant/complex and requiring third party support to gain adequate assurance (Grant Thornton have been engaged), the remaining 6 are being reviewed internally by the Post Offfice central finance team. The current status and findings are:
  - Reviews and discussions have been held with finance managers and business partners to assess data flows, business understanding.
  - For the 6 suppliers reviewed by Post Office, revenue data tied through to support and understanding was gained over data flows. No data issues have been identified to date, however some testing is still ongoing (primarily BGL group). Minimal areas for development have been identified to date.
  - The reviews of the suppliers by Grant Thornton are ongoing. The status across these is that initial discussions have been held, information requests have been submitted and field visits for in-depth testing have begun. The aim is for completion of the work as part of the year end.

POL00423454

Appendix 1: Status of Telecoms specific actions (1 of 2)

	Actions	Who	When	Update	Status
1. Ageing assessment: Identification and scrutiny of the Line rental accused revenue balance would have been facilitated by an effective aging analysis. It was recommended that Post Office engage with Fujitsu to provide a regular report					
Action 1.1	Design and implement an ageing analysis for accrued and deferred balances	CS	Mar 19	Report has been successfully tested and is moving into the production environment for March delivery ahead of year end.	Amber
2. Independent checks: Post Office should develop a further process of periodic review of the information within the Fin11 report to other trends and balances.					
Action 2.1	Implement regular minuted meetings, with actions) between Finance and the Telco business team to review in detail the balances and movements in the Fin11 report (and the Fin2 and Fin 15 reports) versus market, Post Office activity, business logic and P&L performance and "proof in total" reconciliations.	CS / MS	Q4 18/19	Meetings implemented and diarised twice monthly going forward	Closed
Action 2.2	Formally implement "proof in total" checks at FJ on the daily updates to the Data warehouse (e.g. Number of active accounts; total customers). Detail and confirmation to Post Office as part of the regular daily confirmation	CS / AG	Closed	Implemented	Closed
3. Impact on other Reports: As PwC's work focused primarily on the level of accrued revenue, they also recommend that any potentially misleading statements within the regular monthly reporting commentary should be identified and considered.					
Action 3.1	Weekly Telco Report to be expanded to include details of ageing, deferred and accrued expenditure and income for review	CS / AG	Mar19	Dependency on Ageing report (see 1.1 above)	Amber
Action 3.2	Follow-up on areas highlighted in PwC's report on Fin15	CS / MS	Closed	Minor issued identified and confirmed as one off	Closed
Action 3.3	New balance sheet review procedures to be put in place with a focus on reconciliation and supportable analysis back to analytics	CS / MS	Closed	Implemented form P6, with in depth CFO reviews at P3, P6, P9 and P12 each year	Closed
4. Supplementary Reporting: PwC noted that they were made aware of additional "drill down" reports that are available but those reports did not appear to be in regular use. The additional level of detail contained therein may have assisted in the timelier discovery of the misstatement					
Action 4.1	Investigate "drill down" reports to determine if useful	CS	Closed	The information is already in regular use, including the Telephone Rental Drill Down which was highlighted to by us to PwC.	Closed

POL00423454

Appendix 1: Status of Telecoms specific actions (2 of 2)

	Actions	Who	When	Update	Status
5. Risk Assessment: Post Office should develop guidance to support the risk assessment that takes place as part of the monthly balance sheet review. This will help assist in a more rigorous and consistent approach across the business.					
Action 5.1	Develop and formalise a more rigorous monthly balance sheet review process that is consistently applied	MP / CS	Closed	The monthly balance sheet review has evolved, with emphasis moving from "explanations" to "proofs" particularly in accruals and prepayments. This has now been formalised and implemented, with in depth CFO reviews at P3, P6, P9 and P12 each year	Closed
Action 5.2	Identify all the areas where reliance is placed on third party information and develop appropriate control and assurance frameworks around them.	MP / CS	For y/e 18/19	Work is underway for completion for year end.	Green
6. Data Retention: Post Office should insist on a level of data retention from its suppliers to ensure that any future errors are identified and preserved to allow any re-performance where necessary.					
Action 6.1	Determine ways to obtain access to previous versions of the data warehouse	CS / MS	Closed	Discussions with FJ indicate that retention of old Data warehouse versions is not feasible. In mitigation we are maintain our own archives of the key reports	Closed
7. Data integrity: POL should consider the contractual responsibility for confirming the accuracy of the data within the Fujitsu data warehouse.					
Action 7.1	Review contractual responsibility for accuracy of reporting	CS	Closed	Review confirms that FJ has no responsibilities for the "FIN" suite of reports as these were created for Post Office (which signed them off) post-contract. Lessons learned will be incorporated into the for the up-coming procurement	Closed

POL00423454

Cyber Security Update

Authors: David Meldrum/Mick Mitchell Sponsor: Rob Houghton Meeting date: 25 March 2019

Executive Summary

Context

This report provides a short update on the progress with the Security Strategy that was shared with ARC in January 2019, and an update on the management of recent security incidents that have occurred.

Questions this paper addresses

- What progress have we made on implementing the Security strategy?
- What is the progress of the implementation of Archer?
- What remedial activities have we carried out as a result of the recent security incidents that have occurred?

6.1

Conclusion

1. We continue to make progress with our Security Strategy. We have prioritised our investment around 3 key areas – improving the reach and capability of the SOC, including improving our Computer Security Incident Response Team (CSIRT); focusing on improving the management around Data Security including Data Leakage Prevention (DLP); and improving the management and assurance of compliance of our 3rd parties. Solid progress has been made in these 3 areas already (see below) and an investment case will be presented for further funding in March. Furthermore, the current Deloitte review of Cyber and Information Security seems to validate the priorities highlighted in the Security Strategy.
2. Whilst RSA Archer has been implemented for the Security Operations Centre for managing security incidents, the rollout of the additional risk modules including third party assurance has not been agreed or prioritised at present. Further work is required with the Risk function on the best way forward.
3. Since December 2018, we have been the subject of 3 security incidents which have been actively managed. In addition, we have carried a pre-emptive phishing exercise across the organisation to raise awareness of the dangers of email phishing attacks. All of the above events have further validated the priorities we have set for our security strategy, especially around the need to improve our SOC and CSIRT capability.

Input Sought

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

POL00423454

Report

What progress have we made on implementing the Security strategy?

1. Since the last ARC, we have prioritised our major strategic efforts into three themes and we are progressing activities in these areas:
    a. Improving the coverage and capability of the new security operations centre (SOC), including improving our coverage, diagnostics and response capability (CSIRT). The SOC is initially covering the base use cases from our 4 major suppliers and we will extend these use cases, and pick up event logs from other essential suppliers applications. We will also introduce other areas not currently covered such as Payzone. Recent incidents have demonstrated that we need to improve our response process to incidents (CSIRT).
    b. Improving our data security protection, which is protecting our data from leakage through people, processes, and technology/tooling. We have focussed on understanding our unstructured data assets discovery and improving governance on password improvements and Phishing awareness.
    c. Improving the governance and assurance of our IT security posture over our 3rd parties to ensure they are not exposing POL to a possible breach. We have commenced regular Security reviews with our major suppliers to assure they are governing themselves and their 3rd parties. This has already improved the security posture of the services we receive.
2. The current Deloitte review validates the priorities indicated above, with no additional headline items being articulated in the review so far. We continue to keep close to the outputs of this review and will amend our plans accordingly if this position changes.
3. There remain some activities that require funding, which we have prioritised and are progressing for investment, which is in italics in the table below.

Initiative	Time Line	Status	Outcome
Recruitment of CISO	January –April 2019	Inflight	Recruitment of Group CISO to provide added focus on end to end security activity
Multi-factor authentication	November 2018	Completed	Ensuring all remote login's to Post Office environment requires a multi-factor authentication code
Security Operations Centre Go-Live	November 2018	Completed	Centralised security management into joint Verizon / Post Office Security Operations Centre
Recruitment of SOC Lead	January 2019	Completed	Recruitment of Post Office SOC Lead to drive continual improvement
Creating Post Office CSIRT	March 2019	Inflight	Cyber Security Incident Response Team to manage security incidents and issues
Password Audits	December 2018 – March 2019	Completed	Proactive cracking of Post Office password directory to identify scale of issue with weak internal passwords
Disabled all users with weak Passwords	December 2018- onwards	Completed/Ongoing	Disabling all users found to have a weak password. Being reviewed on a weekly basis.

POL00423454

Password Strength Tool Deployment	Go Live March 2019	Inflight	Subsequent deployment of password strength tool, enforcing use of strong passwords
Microsoft Advanced Threat Analytics	Commenced February 2019	Inflight	Security insight on employee office 365 security – multiple logins in different locations, login whilst on leave etc
Varonis Data Discovery Phase 1	February 2019	Completed	Proactive scan of our active directory and share point environment to identify scale of unstructured data
Varonis Data Discovery Phase 2	March 2019	Inflight	Wider scan and auto-classification of data based on the results of Phase 1
Proactive Phishing Campaigns	February 2019	Continuous	Measuring the susceptibility of Post Office user base to simple phishing campaign
Red Teaming exercise	October 2018	Completed	Proactive Ethical hacking exercise simulating internet-based attack of Post Office
Deloitte Audit	January onwards	Completed/Ongoing	End-End Security assessment against industry standards and reviewing progress made in 2016 Deloitte Audit
Symantec Endpoint Protection Upgrade	Commenced February 2019	Inflight/Complete End of March 2019	Improving and updating the anti-virus and laptop protection suite for Post Office end users
Culture and Communications	January 2019	Inflight	Regular messaging from Post Office leadership highlighting expectations around key security themes
Data Security Transformation Programme	December 2019	Inflight	Launched to deliver holistic data classification, protection and management
Third-party governance commenced	January 2019	Inflight	Measuring and managing the compliance of our 3rd parties to internal security policies and standards
Security Enterprise Risk Management	February 2019	Completed	Quantifying and managing residual risk to report to ARC
Data Loss Prevention Suite (DLP)	*Commencing April 2019*	*Business Case Planning*	*To automatically prevent the egress of confidential or sensitive data from Post Office*
Data Classification Tool	*Commencing April 2019*	*Business Case Planning*	*Users will be forced to security classify documents before they can save/print – enabling the DLP tooling*
Security Operations Centre Enhancement	*Commencing April 2019*	*Business Case Planning*	*Ensuring full coverage of all critical systems and services in the SOC*
Mobile Device Management Enhancement	*Commencing April 2019*	*Business Case Planning*	*Ensuring remote Find / Lock / Wipe for all mobile devices within Post Office*
Archer Risk Management Platform	*Commencing April 2019*	*Business Case Planning*	*Expanding the current use of Archer within the SOC into wider security management like 3rd Party assurance*

What is the progress of the implementation of Archer?

4. The initial implementation of Archer as part of the Security Operations Centre (SOC) has completed and the SOC Analysts are currently using the platform for managing security incidents that are raised from the Post Office SIEM (Security Information and Event Management) tool.

5. The expansion of the Archer tool to encompass third party assurance and security controls assurance across the Post Office environment is currently being discussed as part of the strategic risk based approach for the implementation of the security transformation programme. We need to reach an agreed way forward with the Risk function on whether we roll out Archer for Governance, Risk and Compliance (GRC) or use another tool for this.

POL00423454

What remedial activities have we carried out as a result of the recent security incidents that have occurred?

6. At the end of December 2018 we were alerted to 50 PO accounts being available through an Iranian state exploit of multiple companies by the National Cyber Security Centre (NCSC). All 50 accounts had weak passwords and upon notification they were all promptly locked down and forced to use strong passwords.

7. At the end of February the NCSC alerted Post Office to inform that an extract of our Active Directory data - in other words the collection of users that access our email and other systems - is being offered for sale on the internet. The data for sale includes 10000 employee user names, office location and department, but not passwords. The exploit would have likely come from one of our accounts being compromised or a dissatisfied/ fraudulent employee. We have currently discovered no further breaches. Most of this data is publicly available. We continue to actively monitor this incident for any breaches.

8. Also at the end February Verizon Cyber Risk Program advised Post Office that a collection of 29 billion stolen users' credentials (usernames and passwords) had been published in the Dark web in January. From these stolen users' credentials there were 40 that appeared to be from the Post Office. Multiple threat actors claimed to be the source of the data, and were distributing these databases throughout the dark web. The source of the accounts were not obtained from Post Office systems rather from users registering for external non-work related services (e.g. utilities, myfitnesspal etc) and those systems had been compromised. As a precaution, those 40 accounts were disabled and their passwords were changed. A note was sent to all Post Office employees to reiterate the importance of strong passwords and not to register for non-corporate services and applications.

9. In parallel to these events we are now running a number of proactive activities in the Security Operations area to increase our security posture. Examples of these activities are:

    a. We have started to build a strong CSIRT checklist to improve our response to security incidents.

    b. Regular audits of our password database have shown a number of weak passwords, which have been changed.

    c. Regular audits and disabling of administration rights on devices that do not require administration rights.

    d. IT Security ran a phishing campaign in February to determine the level of awareness to potential malicious emails. During the campaign approximately 20% of Post Office employees clicked on the malicious link which in a real phishing campaign could lead to Malware being installed in the Post Office estate. Those employees who clicked on the link are required to complete phishing awareness training so that in the future they are able to detect and report phishing emails.

POL00423454

e. We have increased the analytics around the O365 estate to monitor unusual user behaviours (e.g. multiple logins from different locations at the same time).

f. We are reviewing the capability of our threat intelligence partner, Digital Shadows, in light of the above incidents as we need to improve our external threat intelligence.

g. We have identified around 140,000 "stale" (not accessed within 60 days) files containing sensitive data and about 14,000 sensitive files being shared with external users. We are now looking at ways to classify and control these files more actively.

h. We have increased our contact with the National Cyber Security Centre.

POL00423454

Back Office Transformation

Author: Benjamin Cooke **Sponsors:** Rob Houghton, Alisdair Cameron

Executive Summary

Context

In January the board were taken through the Go/No-Go decision. On January 28th we transitioned our Supply Chain operations to Transtrack CWC and financial processes to our Core Finance System (SAP CFS). POLSAP is now an archive. The significant risk from its hardware has been mitigated.

Two areas of concern and manual working were highlighted: our ability to reconcile daily cash movements from Transtrack CWC through to CFS; and delays in the intermediate and permanent solutions for branch cash forecasting.

This paper provides an update on the Go-Live, a summary of progress on the issues, and an overview of other issues faced since Go-Live with a focus Branch impacts.

Questions addressed in this report

1) What is the current project status?
2) What has the impact been on our finance and supply chain operations?
3) How has the lack of a cash forecasting tool impacted Branch cash?
4) What is the impact of Transtrack CWC financial reconciliation issues?
5) What impact has the project had on Branches?
6) Where are we on financials and next steps?

Conclusion

- We are now fully live and have completed a month end on SAP CFS for financials. There have been some teething issues on the Sales-Finance side but limited and managed.
- Daily operations in Supply Chain on Transtrack CWC are taking longer to settle down with basic in-bound and out-bound processing not yet back at pre-go-live pace, but heading in the right direction. Delays in processing inward REMS rose significantly but levels are now back to normal. Tactical issues impacting users have been addressed more slowly than we would like, with Transtrack's development team focused on our larger challenges.
- Reverting to standard cash remittances for Branches peaked at an additional £87m of cash in the network. In the second week of March planned cash orders have been reinstated and excess cash has already dropped to £60m. We expect this reduction to continue. The sterling forecast solution will move to parallel run this month.

POL00423454

- Physical cash is counted weekly at all sites and matches Transtrack cash-on-hand figures. A number of initial differences arose but these have been investigated and cleared with support from Internal Audit.
- However, a substantial transactions are not being successfully processed through CWC and into SAP CFS. Initially, we were also unable to make the reporting work, proven before Go-Live, that identified all of the transactions underlying the difference. The reporting issues are resolved, giving assurance that there is no loss and enabling us to identify root cause to prevent new and clear old differences: we can see all the individual transactions "stuck" in CWC.
- Unfortunately the progress that Transtrack is making to identify and resolve the root causes is unsatisfactorily slow, reflecting their limited scale. Accenture and ourselves are assisting with both assessments and skill sharing. Nonetheless, it may well be May/June before we are operating cleanly.
- We are working closely with PwC to ensure that we produce timely, audited accounts. In the Lessons Learnt exercise for BoT we may conclude that the capability of Transtrack, an existing provider, should have received more challenge.

The Report

Current Project Status

Cutover

1. The cut-over weekend was executed successfully. On Monday 28th January, our client settlements were paid manually, and our Bureau Cash Operations were primarily manual both Monday and Tuesday. Beyond that, other than the issues below, we have been operating in our target state from the beginning of February.

Finance Processes (POLSAP Process Migration)

2. In total, our finance teams have raised 185 issues, of which only 31 severity 3/4 issues remain open. One or two clients queried the new invoicing processes. Royal Mail were invoiced two days late but were communicated with throughout.
3. We completed our first month-end on the new systems. However, we have decided to retain erly-life project support remains until after the financial year-end as a precaution. Horizon (and all web/app) sales are now channelled into CFS which uses master data contracts to auto-calculate settlement and billing for every client/product and uses the same data for agents' pay and financial reporting.
4. This month our first system generated product profitability reporting is available in CFS, although it will need some time to fully operationalise.

Strictly Confidential

POL00423454

Supply Chain; Cash Processing

5. Supply Chain operations has been more of a challenge. It took around 4 weeks for basic in-bound and in-bound cash processing to settle down and perform at pre-Go-Live levels. There are indications that we may start to see performance gains, which are being sought. Processes changed most significantly in the area of cash corrections.
6. Data is captured at a more granular level than before, which creates stronger controls and reporting, but caused some initial confusion with manual working in bureau on the first few days, and confusion with stock corrections leading to a back-log of items that needed checking and re-processing. This has taken time to work through alongside our ongoing operations.
7. An initial backlog of corrections has been resolved with help from Internal Audit.

Supply Chain; Cash Forecasting

8. Cash forecasting moved to standard remittances for all Branches (i.e. rather than forecast, they received a set pre-agreed value). At its peak, it increased branch cash by £87m.
9. Calls from Branches reduced during this period as most were over funded. In the second week of March we re-introduced planned cash orders, increasing collections and reducing cash orders. Excess cash has reduced to £60m and should continue to fall.
10. Branch calls have returned to pre-Go-Live levels and feedback from the NFSP is that neither switch has caused undue concern within the network.
11. The sterling cash forecast solution is about to start parallel run and will be evaluated over the coming weeks. As the inventory team become confident in the proposals they will enable more automation. Given this timescale and the need to fund Easter it may be end May before branch cash returns to the £450m level seen after Christmas.

Transtrack CWC Cash-on-Hand to CFS Financial Reconciliation

12. Our biggest challenge Post-Go-Live has been reconciling Transtrack CWC's accurate Cash-on-Hand figures to the values it sends to CFS. A significant number of cash movement transactions occur but fail to make it to the out-bound interface.
13. We knew this pre-Go-Live and had made progress in closing issues. Even though we expected the problem to get worse, the GO decision was made as:
    a. we knew physical cash reconciled to Transtrack local site cash on hand (more on this in following section), and
    b. a model was created that quickly identified all missing transactions for analysis.
14. Following go-live this problem was worse than expected. It's important to note that physical cash still reconciles to Transtrack cash on hand so there is no risk of physical cash loss. However, the model allowing us to identify transactions failed, preventing the ability to pin-point issues and solve root cause.

POL00423454

15. With Transtrack and Post Office resource spread across our sites, supporting operations it took some time for the report failings to be analysed and fully resolved.
16. On Feb 25th we reached our pre-Go-live position of being able to see each missing stock transaction and moved focus to identifying root cause. Resolution has been limited by the size and capability of Transtrack's development team and we are working with Accenture to actively bolster their capability, which will improve our pace of resolution. Current estimates indicate that we will still be closing issues through May/June.
17. At year end there will still be a meaningful difference between the balance on CWC and on CFS. However as the underlying CWC data is supported by weekly cash counts and we have a transaction listing of all stuck transactions, we believe that we can support our accounts. Finance are conducting a mock year-end for cash GLs on Sunday 17th March to test the approach agreed with our auditors and confirm appropriate documentation.

Supply Chain; Physical Cash Counts

18. During this period, Supply Chain have been completing full site cash counts at every location each week. Friday 8th returned a complete match at all sites but one; this had a slight shortage which we expect to be due to an overage the week before.
19. This process took time to get right due to a high number of manual "stock corrections" that occurred during and after go-live. Some of these were user error, many needed to correct actions in the first few days. Not all had adequate paperwork.
20. Our internal audit, supported by external financial audit team have worked with supply chain – reviewing old CCTV footage where necessary – to double check each of these stock corrections. In summary their view is that nothing malicious has occurred and we expect to close the last few in the coming days. Several useful recommendations about our stock correction process have been made that we will look to implement.

Strictly Confidential

POL00423454

Branches Impacting Issues

21. A number of issues faced in project early life support have impacted branches. Each issue is being fully documented through to resolution in a format agreed with the Legal Team, learning lessons from the GLO process.

Issue	Impact	Resolution
Official Postage Product Removed and re-activated wrongly	Branches who claimed Official Postage whilst the default mode was incorrect now have a discrepancy. These transactions are relatively low value hence the average impact per impacted Branch was around £13.	The product was wrongly removed during a large data cleanse. This was quickly realised with the product re-instated, however only half the product was technically re-instated causing the Post Master to make a loss each time they transacted. This was technically corrected after 7 working days. 1093 branches transacted during this period need to complete a reversal transaction to correct. 624 have, 469 are outstanding. All have been contacted and our out-bound call centre will continue to call the 469 until they are resolved.
Manual cash receipting due to: 1. Bureau manual operations 1. Pre-announcement failure	When a Branch receives cash and scans in a pouch the cash received is auto-populated. If this pre-announcement is not available then Branches manually enter cash received. This leads to errors such as selecting the wrong currency, or entering too many "00"s.	In the first 2 days after Go-live our bureau cash operated manually, meaning no pre-announcements were available. Around 500 branches made errors when entering cash receipts. The 17 whose errors were over £50k were informed quickly with the issue resolved within 15 days. In total there were around 150 possible errors being investigated with communications sent to all impacted branches. On 27th Feb the pre-announcement interface failed due to a number range running out in Horizon. This was fixed within 6 days. A report on whether this type of issue could apply to other interfaces is being worked through. Matching of issues and receipts is in progress to determine the number of branches impacted.
Transtrack HQ crash	The Transtrack CWC HQ system crashed twice impacting the inventory team who were unable to get all orders out for the day.	This issue impacted 134 bureau and 200 coin deliveries, the Branches were sent their orders the next day. With a server re-boot the system came back and the root cause is known. The issue was permanently fixed on 18th March date.

Strictly Confidential

POL00423454

Going Forward

22. The project team are preparing project closure reports and continuing to deliver outstanding elements of scope including the archiving of POLSAP, small changes delayed until post-go-live, technical environment close out and continuing to upskill business team super-users on the new processes and systems.
23. Whilst we are unable to forecast precisely when our issues will be resolved we believe that we will complete within the £37.3m cost forecast for a Jan Go-Live that was provided in September. However some of the scope initially planned will not be completed, the largest of these being our future forecasting solution which requires rethinking. Any outstanding scope will go through the diligence of our change funding and prioritisation process. An update on program close our will come to the board in May or June.

Strictly Confidential

POL00423454

Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 25th March 2019

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Audit, Risk and Compliance Committee (ARC) meeting in January and progress on the 2018/19 Internal Audit Plan.

Questions this paper addresses

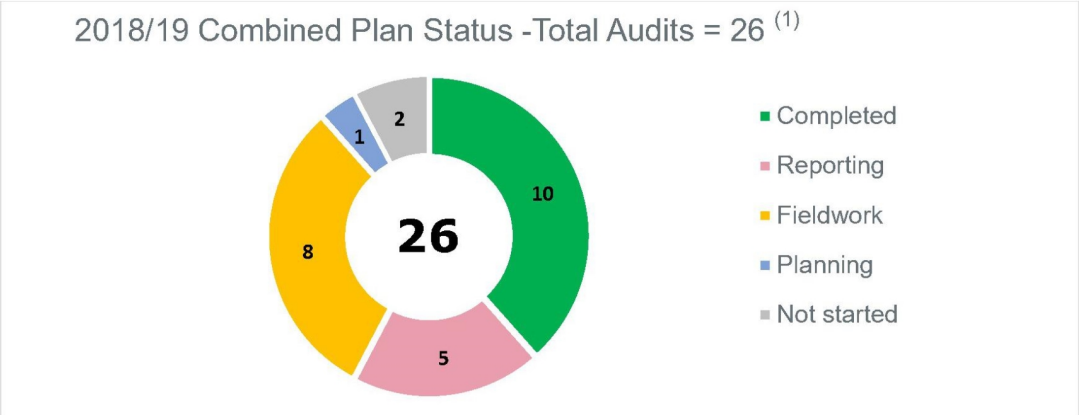
- Is the Internal Audit Plan on track? What progress has been made since the last meeting?
- Do Internal Audit have adequate resources to deliver the Audit Plan?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan:

We are making good progress following the delays experienced in 2018, with 24 of the 26 reviews on track for delivery by the May ARC meeting. The remaining two reviews are change assurance reviews, which are currently being re-assessed in consequence to the change portfolio being reprioritised. Our initial view is that it is too early to review these programmes and that they are likely to be delayed to 2019/20.

One review has been finalised since the January ARC, with five reviews currently in reporting and a further eight in fieldwork. An update on the ongoing Cyber Security Maturity review is provided in paragraph 8. Current delivery progress is as follows:



(1)ARC approved baseline plan for 2018/19 (16 core internal audit reviews & 10 change assurance reviews).

A full summary of the 2018/19 audit plan status is included in **Appendix 1**.

POL00423454

2. Open and Overdue Audit Actions (as at 18 March 2019):

Audit Action Status:	
Open (not yet due)	19
Overdue (<60 days)	0
Overdue (>60 days)	0
Total	19

More detailed information is provided in paragraph 11 of the report.

3. Significant Issues:

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

Input Sought

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

POL00423454

The Report

Changes to plan since January ARC meeting

4. There were no changes made to the audit plan since the January ARC meeting. The re-prioritised plan approved by the ARC is attached as appendix 1.

POMS Audit Plan

5. POL Internal Audit is also responsible for delivery of the audit plan for Post Office Insurance (POMS). Progress with the 2018/19 audit plan is reported at the POMS ARC. All five audits on the plan are now complete or underway:

- Insurance Distribution Directive (IDD) - Readiness Review (Complete)
- Oversight of Appointed Representatives – Phase 1(Complete)
- Nemesis Project - Programme assurance (Reporting)
- Oversight of Appointed Representatives – Phase 2 (Planning)
- MI quality and effectiveness (Planning)

Internal audit reviews completed

6. Since the January ARC meeting we have finalised the review of Bank Account Governance. Our findings and observations are summarised below (the full audit report is included in the reading room):

Bank Account Governance (Ref. 2018/19-14)

Satisfactory

Sponsor:
Al Cameron

Audit actions:

P1	0
P2	1
P3	2
Total	3

Following recent headlines over the material shortfall between Patisserie Valerie's actual and reported financial positions, and investigation by the Serious Fraud Office (SFO), the CFOO has requested that Internal Audit carries out a review of the controls over bank account governance within Post Office.

The audit assessed the design and operating effectiveness of controls in place over all aspects of governance of Post Office bank accounts, including delegated authorities, bank mandates, set up of new bank accounts, restricted access to online banking facilities, monitoring mechanisms and bank reconciliations.

We conclude that the controls over the setting up and management of bank accounts are well established and effective, as a result we have rated this report **Satisfactory**. There is reliance placed upon the Treasury team to operate the controls over bank account set-up and management and work is ongoing to address the lack of detailed process guidance to enable these duties to be covered in case of absence or turnover. The Treasury Policy is signed off by the CFOO and is subject to annual review (and re-approval by the ARC).

The audit took longer than anticipated due to resource constraints within the Treasury team and with the previous TR&C manager leaving, and his replacement undergoing his induction, there is work being undertaken to ensure continuity and handover of the key banking contacts and relationships.

Management Comment provided by Al Cameron

Thanks to Internal Audit for a timely and helpful review.

8.1

POL00423454

Internal audit reviews in reporting

7. The following internal audits have been completed and the reports are currently being cleared with management:

	Review	Status / Remarks
1	Branch Hub (Change Assurance)	Final draft report for management comment
2	Network Reporting	Final draft report for management comment
3	Agent Remuneration	Final draft report for management comment
4	Cyber Security	Draft report – see par 8 for progress update
5	Contract Management (IT)	Final draft report for management comment

Update on Cyber Security Maturity Assessment

8. Following previous audits of information security in 2013 and 2016 and a red-team exercise in September 2018, the Board have expressed a desire to understand the level of progress towards increased Cyber Security maturity.

9. Deloitte conducted an initial review of the 34 cyber security capabilities, using the Deloitte Cyber Security Framework (CSF) in January 2019. This high level assessment was intended to provide a rapid view of areas for a "deep dive" second phase assessment. The findings from phase 1 identified 19 domains to be assessed as priority, however, it was decided that establishing a baseline maturity across all 34 domains would be more desirable and would assist management in prioritising remedial actions.

10. The phase 2 review has experienced some delays and although the fieldwork is substantially complete, Deloitte still have to agree with management appropriate maturity targets and remedial action plans. As a result, the final maturity assessment and action plan were not ready at the time of writing this report. We have, however, attached a preliminary report as appendix 2 and will endeavour to circulate the finalised report ahead of the ARC meeting if possible.

Updates on Internal Audit Open and Overdue Actions

11. Audit actions are generally being completed on time. As at 18 March there were 19 open actions, none of which were overdue.

Audit Action Status:	BAU	Change	Total
Open (not yet due)	18	1	**19**
Overdue (<60 days)	0	0	**0**
Overdue (>60 days)	0	0	**0**
Total	18	1	**19**

END OF REPORT

POL00423454

Appendix 1 – Re-prioritised Plan (As agreed with ARC on 30 October 2018)

2018/19 Internal Audit Plan - Status as at 18 March 2019

No.	Title/Subject	Sponsor	Original / Addition	Timing	Status / Rating
Internal Control Reviews					
1	Product Risk Review (Postal Orders)	O. Woodley	Original	April	Needs Improvement
2	Employee Expenses	A. Cameron / M. Kang	Original	April	Unacceptable
3	Procurement Fraud Investigation	A. Cameron	Addition	May	Not Rated
4	Month-end Close Process	A. Cameron	Addition	Nov	Satisfactory
5	MoneyGram Compliance	O. Woodley	Addition	Sept	Satisfactory
6	Contract Management (IT)	R. Houghton	Original	Oct	Final Draft Report
7	Whistle-blower Process	J. MacLeod	Original	Oct	Satisfactory
8	Opening of Bank Accounts	A. Cameron	Addition	Nov	Satisfactory
9	FS Training & Competence	O. Woodley / M. Kang	Original	March	Planning
10	Cyber Security	R. Houghton	Original	Jan	Draft Report
11	IT Control Framework	R. Houghton	Original	March	Fieldwork
12	Financial Control Framework	A. Cameron	Original	Jan	Fieldwork
13	Payroll	M. Kang	Original	Feb	Fieldwork
14	Client Settlements Process (Interim Controls)	A. Cameron	Original	Jan	Fieldwork
15	Agents Remuneration	A. Cameron	Original	Jan	Final Draft Report
16	Network and SGEI Reporting	D. Smith	Addition	Feb	Final Draft Report
17	Procure to Pay	A. Cameron	Original	Q4 / Q1	Postpone[2]
18	Branch Cash Forecasting & Management	A. Cameron	Original	Q1 19/20	Postpone[1]
19	Supply Chain Management	A. Cameron	Original	Q1 19/20	Postpone[1]
20	Digital Strategy & Capability	O. Woodley	Original	2019/20	Postpone[2]
21	Online Sales	O. Woodley	Original	2019/20	Postpone[2]
22	Data Privacy (GDPR Follow-up)	J. MacLeod	Addition	Q1 19/20	Postpone[2]
Change Assurance[3]					
1	Change Excellence (Trafalgar)	R. Houghton	Governance	May	Advisory Report
2	DMB Strategy	D. Smith	Programme	July	Satisfactory
3	Branch Hub (Agents Portal)	D. Smith	Programme	October	Final Draft Report
4	Investment Funding Controls	R. Houghton	Governance	November	Needs Improvement
5	Payzone Integration (Panther)	D. Smith / A. Cameron	Programme	Jan	Fieldwork
6	Digital Identity Services	M. Edwards	Programme	Feb	Fieldwork
7	Digitising Mails	D. Smith	Programme	TBC	Being assessed
8	Payment Technology Upgrade (PCI)	D. Smith	Programme	TBC	Being assessed
9	Change Excellence (Follow-up)	R. Houghton	Governance	March	Fieldwork
10	P2C Belfast Exit	R. Houghton	Programme	March	Fieldwork

[1] Delay until after BOT programme is complete and new controls embedded.
[2] Postpone due to process still bedding down and maturing (GDPR) / restructuring (Digital & Online) / remediation (P2P).
[3] The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2018/19 at the time. The list is being reviewed and updated on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum' projects.

POL00423454

Appendix 2

Deloitte Assessment of Post Office Ltd Cyber Security Maturity - Phase 2 Pre-Report Memo

Introduction

Deloitte assessed the information security posture at the Post Office Ltd (POL) in 2013 and 2016. POL has made progress in addressing the points raised in those assessments and there are a number of key strengths; but some actions remain outstanding.

Deloitte conducted a further high-level review of 34 cyber security capabilities across POL using the Deloitte Cyber Security Framework (CSF) during January 2019. The output from this work (known as phase 1) sought to gain a rapid view of areas for further investigation and assessment. The output of phase 1 activity has been reported in a Deloitte memo previously.

This memo relates to a further detailed and evidenced based review of those 34 cyber security capabilities assessed in phase 1. During phase 2, the in-depth assessment comprised of interviews with key POL stakeholders and detailed documentation review. The output from this process is a validated maturity score across the 34 cyber security capabilities, the provision of two industry benchmarks against which POL cyber capabilities may be compared and detailed recommendations, which if implemented, will take POL to target maturity as selected by POL. The phase 2 outputs also provide the basis of a repeatable assessment of cyber maturity for the POL so that cyber security maturity can be continually tracked as improvements are delivered over time.

8.1

High-Level Summary of Cyber Security Maturity Scores

Deloitte Cyber Strategy Framework Domains	Phase 1 Un-validated Maturity Score	Phase 2 Validated Maturity Score	Average Maturity (Global Retail)	Average Maturity (Global FS)
Governance	1.9	2.4	2.4	2.7
Secure	2.0	2.1	2.5	2.7
Vigilant	1.8	2.0	2.5	2.5
Resilient	1.9	2.1	2.4	2.7

POL00423454

Overview of Key Strengths

The key areas of strength identified during phase 2 are outlined below:

Governance Structure

POL has mature security teams who discharge security responsibilities across IT, Information Security, and Information Protection and Assurance. Their work is supported by senior internal stakeholders and a network of working groups including the Information Security Committee (ISC), Cultural Committee and Cyber Risk Assessment Forum (CRAF), which all feed into the Audit and Risk Committee, and ultimately, the Post Office Board. This ensures that there is a route for escalation of cyber issues and sharing of cyber related information across the organisation. There is also a good understanding of the regulatory requirements which underpins this governance structure across the organisation (including PCI, GDPR and FCA, etc.).

Security Policy Coverage

POL has a comprehensive suite of wider security policies which leverage best practice from industry standards (such as NIST and ISO 27001). All policies are available through a centralised location on the Intranet or Horizon. All policies are reviewed annually or as appropriate in accordance with key POL or security developments, such as GDPR. Although this is a strength, there is further policy development that can be undertaken to increase control effectiveness across the organisation.

Cyber Risk Discussion and Information Sharing

POL is proactive in raising and responding to risk(s) identified through the involvement of relevant stakeholders, formally captured via the Cyber Risk Assessment Forum (CRAF), risk registers and an easily digestible colour coded (red/amber/green) risk priority matrix.

Business continuity management and Disaster Recovery

An experienced Business Continuity Management (BCM) and Disaster Recovery (DR) team understands the business and its priorities. Business Continuity Plans (BCPs) and DR plans are in place for each business area and relevant testing exercises are conducted. Post incident reviews are undertaken following incidents and lessons are fed back to enable continuous improvement.

Physical Security of Cash in Transit and Depots

The physical security procedures for handling cash both in transit and at depots are extremely robust and effective in accordance with Bank of England standards and other relevant legislation. Controls are based on a layered approach, and reviewed and updated as required as per the latest developments in requirements and technology. Regular testing and lessons learned are captured through spot checks and inspections.

POL00423454

Overview of Key Opportunities

The key opportunities identified during the assessment are outlined below:

Crown Jewels

During the assessment, a provisional list of POL crown jewels was developed to provide input to the Cyber Strategy Framework assessment. Developing an understanding of those crown jewels that are critical to the business, as well as the confidentiality, availability and integrity requirements, is essential in order to realise the strategic benefits of any security programme. The cyber security strategy and resources can then be aligned to protect these crown jewels accordingly.

Risk Appetite

POL is currently operating from Risk Appetite statements dating back to 2015 and these are currently being reviewed. In order to clearly set the strategic direction and basis of all risk-based decision making an opportunity exists to formalise and promulgate these statements at the earliest opportunity to enable clear understanding across the business.

Cyber Metrics

During the assessment evidence was presented of a suite of Key Risk Indicators (KRIs) that are used to inform risk discussions and information sharing across the business. There is an opportunity to review and evolve these to capture all cyber related factors such as coverage of cultural activities, incident response metrics and threat intelligence key performance indicators (KPIs) and KRIs. Appropriate cyber dashboards can then be regularly presented at Board level to better articulate risk, and demonstrate return on investment and benefits realisation of the cyber strategy.

Threat Intelligence Capability

POL is currently developing its Security Operations Centre (SOC) to coordinate and correlate security event monitoring across the enterprise. In parallel its threat intelligence capability is being evolved and grown. Significant opportunities exist to develop a formal Cyber Threat Intelligence (CTI) programme, CTI model and threat library in order to inform decision making across the business both proactively and real-time.

Incident Readiness and Response

Significant work is being undertaken in the area of incident readiness and response and opportunities exist to formally document all related process and procedures. The integration of incident response capability to business continuity management is worthy of attention and mutual exercising and testing in order to ensure effectiveness of procedures and escalation paths/decision making.

Insider Threat Programme

The Post Office has identified that the threat of a malicious insider is one of the top two threats it faces. Consequently, an opportunity exists to develop an effective insider threat programme, with relevant key risk indicators identified and in partnership with all key stakeholders (including human resources) to mitigate against this threat.

POL00423454

Cyber Security Maturity

Now that the Phase 2 assessment fieldwork is complete, preliminary capability maturity scores are reported. It should be noted that those capabilities marked with a * within the table are still subject to validation and quality review and may change.

The maturity level scoring is aligned to the descriptions in the table below.

Level 1	Level 2	Level 3	Level 4	Level 5
Initial	**Repeatable**	**Defined**	**Managed**	**Optimised**
Capability is typically undocumented and in a state of dynamic change, tending to be driven in an ad-hoc, uncontrolled and reactive manner. Basic/Early level of implementation.	Capability is performed on a regular basis but is not formalized or consistent. Coverage is not agreed or comprehensive. Mostly at a standard level of implementation, but still basic in places.	Capability is formally documented, with an agreed ownership and scope, and is used throughout the majority of the organization. Standard level of implementation.	Capability is actively maintained, and performance is regularly reported in a format that can be actioned. Advanced level of implementation in places, with almost full coverage.	Capability is continually improved through both incremental and innovative changes. Advanced/industry leading implementation and full coverage.

The table overleaf illustrates the unvalidated phase 1 and validated phase 2 capability maturity scores. Also presented is benchmark data drawn from: 1) large retail businesses including global retailers and, 2) financial services benchmark drawn from global banks and investment houses. In addition to the maturity scores there are a number of significant change programmes in-flight that are scheduled to deliver within the next 6-12 months at POL, and which if delivered, are expected to have an upward impact on current cyber security maturity levels across the capabilities.

Recommended Next Steps

Based on the output of the current assessment the following is advised:

1. Select cyber capability target maturity levels. Target maturity levels will be selected by POL management, supported by Deloitte based on the nature of POL's business model, industry benchmarks and Deloitte suggested target maturity levels.
2. Implement a programme of cyber security activity based upon the recommendation made, whilst continuing to deliver the improvement activities in pipe-line to realise key benefits for POL.
3. Schedule an interim further independent cyber maturity assessment review at 6 months and a more detailed assessment at 12 months to validate progress against selected target maturity.

POL00423454

Deloitte Cyber Security Maturity Review - 18 March 2019

Domain	Sub-domain	Capabilities	Phase 1 Un-validated Maturity Score	Phase 2 Validated Maturity Score	Average Maturity (Global Retail)	Average Maturity (Global Financial Services)
Governance	Cyber security management	Strategy & operating model	1.8	2.3	2.3	2.4
		Policies, standards & architecture	2.0	2.7	2.4	2.9
		Cyber risk culture and behaviour	1.8	1.9	2.4	2.6
		Cyber risk mgt, metrics & reporting	2.0	2.7	2.3	2.8
Secure	Extended Enterprise and Infrastructure	Cloud security	2.3	2.4	2.6	2.4
		Third party risk management	2.2	2.5	2.5	2.7
	People & Workplace	Human resources security	2.5	1.6	2.3	2.8
		Physical security	2.2	2.6	2.8	3.1
	Identity & Access management	Identity lifecycle management	1.5	1.8	2.5	2.9
		User access control	2.5	2.9	2.6	3.0
		Role based access control	1.5	1.9	2.6	2.8
		Privileged user access control	2.0	2.6	2.6	2.6
	Applications	Secure Software Development Lifecycle	2.5	1.7	2.6	2.6
		Post-development application protection	2.5	2.4	2.3	2.6
	Infrastructure	Asset management	1.5	1.6	2.5	2.6
		System security	2.0	2.1	2.4	2.6
		Malware protection	2.5	2.4	2.7	3.1
		Network security	2.0	2.3	2.4	2.7
		End-user device security (CD)	2.0	2.5	2.4	2.7
	Data	Data loss prevention	1.2	1.6	2.2	2.3
		Encryption	2.0	2.3	2.3	2.6
		Information lifecycle management	1.5	1.8*	2.3	2.4
		Data privacy	2.0	2.1*	2.4	2.6
		Information classification	1.0	1.6*	2.3	2.3
Vigilant	Vulnerability identification	Penetration testing & vulnerability scanning	2.0	2.2	2.2	2.7
	Threat Intelligence	Cyber threat intelligence (CTI)	1.2	1.6	2.6	2.4
		Brand protection	1.5	2.0	2.8	2.5
	Security Operations (SOC)	Security event monitoring	2.0	2.1	2.4	2.4
		Patch & vulnerability management	2.2	2.4	2.4	2.9
		Cyber analytics	N/A	1.2	N/A	N/A
		Security platform administration & operations	2.0	2.2	2.5	2.3
Resilient	Incident management	Incident & crisis readiness	1.8	2.0	2.4	2.5
		Incident response	1.8	1.6	2.5	2.6
	Business Resilience	Business continuity management and recovery	2.0	2.7	2.3	3.0

**** indicates that these scores remain subject to validation.***

8.1

POL00423454

POST OFFICE LIMITED DECISION PAPER

AUDIT, RISK & COMPLIANCE COMMITTEE

Internal Audit Plan 2019/20

Author: Johann Appel Sponsor: Jane Macleod Meeting date: 25th March 2019

Executive Summary

Context

1. The Post Office annual risk-based audit plan for 2019/20 has been prepared in accordance with the applicable requirements of the Internal Audit Charter as approved by the ARC in March 2017, as well as the professional standards of the Chartered Institute of Internal Auditors (CIIA).

Questions addressed in this report

2. What processes, activities and programmes should be assured by Internal Audit in 2019/20? Does the proposed plan focus on the right priorities to support the Post Office strategic objectives?
3. What are the resource requirements to deliver this audit plan and how much will it cost?

Conclusion

4. An integrated audit plan has been prepared to provide assurance over principal business risks and significant change activities. The proposed plan can be summarised as follows:

Category	Number of audits	Estimated effort (days)		Co-source cost
		Total	Co-source	
Core Internal Audit	18	613	217	£235k
Change Portfolio	10	315	250	£271k
Total	**28** [N1]	**928**	**467**	**£506k** [N2]

[N1] 2018/19 plan was for 26 audits.

[N2] 2018/19 Co-source cost budget was £560k. The cost reduction of £54k has been achieved by hiring an in-house IT auditor, partially off-set by the cost of providing two additional audits. Overall comparative cost will remain broadly unchanged or marginally favourable compared to the prior year.

Input Received

5. The proposed Internal Audit Plan for 2019/20 was developed with input from Post Office GE and the wider business. The plan was then reviewed and discussed by Post Office Risk & Compliance Committee (RCC), who considered the proposed reviews to individually and collectively represent an appropriate programme to support management in their activities and to provide assurance to the Audit, Risk & Compliance Committee (ARC) over key risks to Post Office.

Input Sought

6. The committee is asked to review and approve the proposed internal audit plan for 2019/20.

POL00423454

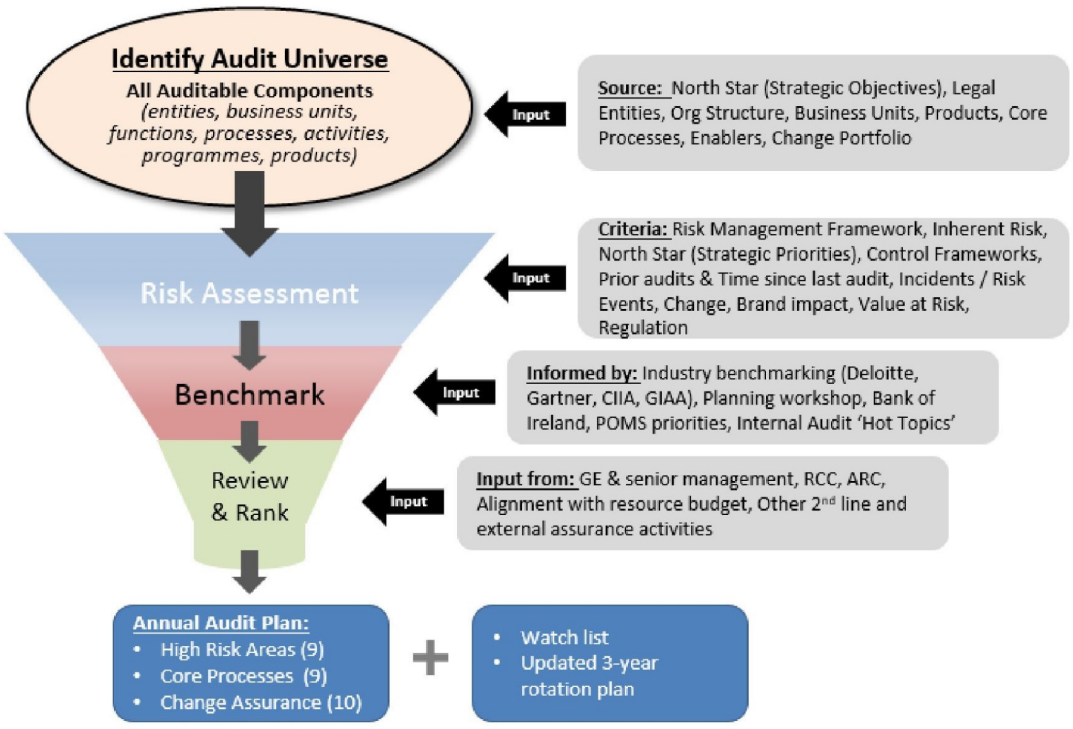
Detail

The Planning Context

7. Post Office risk profile is impacted by continued and significant internal change, increased regulatory scrutiny and market pressures. The 2019/20 Internal Audit plan is designed to provide assurance over the organisation's principal risks, core processes and material change activities.
8. As of 2017/18 we have introduced a three year rotation plan for core processes (refer par. 17). Core processes are usually mature and generally expected to be well controlled, but warrant cyclical validation due to their pervasive nature and criticality to the business. The 2019/20 plan includes the third and final tranche of core processes to be reviewed over a three year period.

The Planning Process

9. The following diagram depicts the process we followed to identify, assess and prioritise the processes and activities to be assured in 2019/20:



The Planning Results

10. The proposed list of audits was discussed with GE members and senior management and their feedback has been incorporated.
11. The tables below outline the proposed audits to take place in 2019/20. Internal and external events may cause priorities and risk profiles to change, and management may have additional requests during the year for advisory support or audit assistance. In consequence, we may consider amending the plan as the year progresses. We will also re-assess and refresh the plan at mid-year to ensure it remains relevant. We will seek ARC approval for all material changes to the plan.

POL00423454

12. **Table 1** represents the baseline plan for internal control reviews, of which the target delivery is 18 reviews. High level audit scopes for each review can be found in Appendix 1.

1. Internal Control Reviews – Target = 18 reviews			
Rank	**Proposed Review**	**GE Sponsor(s)**	**Timing**
1	Procure to Pay	Interim CFO	Q1
2	Branch Cash Forecasting	Rob Houghton	Aug
3	Supply Chain (CViT)	Rob Houghton	Aug
4	Accounts Receivable	Interim CFO	Flex
5	Agent On-boarding	Debbie Smith & Rob Houghton	Q4
6	Pensions Follow-up	Mo Kang	May
7	Employee Expenses Follow-up	Mo Kang & Interim CFO	July
8	Branch Banking Framework	Debbie Smith	Q3
9	Sales (Savings Accounts)	Owen Woodley	Q3
10	Vetting / Fit & Proper	Jane MacLeod & Rob Houghton	Flex
11	Effectiveness of Risk Management Framework	Jane MacLeod	Flex
12	CFS Controls (Post Back Office Transformation)	Interim CFO	Q2
13	Effectiveness of Compliance Function	Jane MacLeod	Flex
14	Telecoms Customer Billing	Owen Woodley	Q1
15	Data Privacy (incl. follow-up of GDPR)	Jane MacLeod	Q1
16	Cyber Security Follow-up	Rob Houghton	Q2
17	Payzone Control Framework	Debbie Smith	Q2
18	FS Branch Sales	Owen Woodley & Debbie Smith	Flex

13. **Table 2** represents reviews of significant change activities. The baseline plan is for 10 change assurance reviews. This is an indicative list based on the current change portfolio and will be reviewed and updated continuously as the portfolio of change programmes develops and the risk profile changes. The draft plan includes four thematic reviews focusing on programme governance (e.g. gating effectiveness, benefits realisation). The thematic reviews will be balanced with the need to provide assurance over individual change programmes – this could be assurance at a point in time or ongoing / real time assurance, depending on the project.

POL00423454

2. Change Portfolio / Programme Assurance – Target = 10 reviews			
Rank	**Proposed Review**	**GE Sponsor**	**Timing**
1	Investment Funding Controls follow-up (Governance)	Rob Houghton	Jul / Aug
2	Effectiveness of 2nd line Programme Assurance (Governance)	Jane MacLeod	tbd
3	Benefits Realisation (Product Realisation) (Governance)	Rob Houghton	tbd
4	Effectiveness of the Gating Process (Governance)	Rob Houghton	tbd
5	Placeholder (Governance / Programme review)	Rob Houghton	tbd
6	Belfast Exit (phase 2)	Rob Houghton	Sept
7	Data Governance Programme (Record management)	Rob Houghton	tbd
8	PTU (PCI Compliance)	Rob Houghton	tbd
9	Digitising Mails	Debbie Smith	tbd
10	Identity Services (Follow-up)	Owen Woodley	tbd

14. **Table 3** is our 'watch list' of additional areas for consideration during the year, should either the assurance needs for the priority areas decrease or risk levels for items on our watch list increase. The watch list will also inform the 2020/21 audit plan.

	Topic / Area
1	Identity and Access Management (incl. Joiners / Movers / Leavers) follow-up
2	Contract Management (Including revenue contracts such as POCA)
3	Effectiveness of IT Security Operations (2nd Line)
4	Digital Strategy
5	SuccessFactors (Change Assurance of Phase 2)
6	MoneyGram (Product Risk)
7	ITDR
8	Brand Protection Strategy / Controls
9	Credit Card (New Provider)
10	Online Sales
11	Digital Identity (Control Framework / Operational Controls)
12	Business Continuity Management follow-up

POL00423454

Post Office Insurance (POMS) Audit Plan

15. The table below shows the proposed audit plan for Post Office Insurance (POMS). The plan is subject to approval by the POMS ARC and is included for information only.

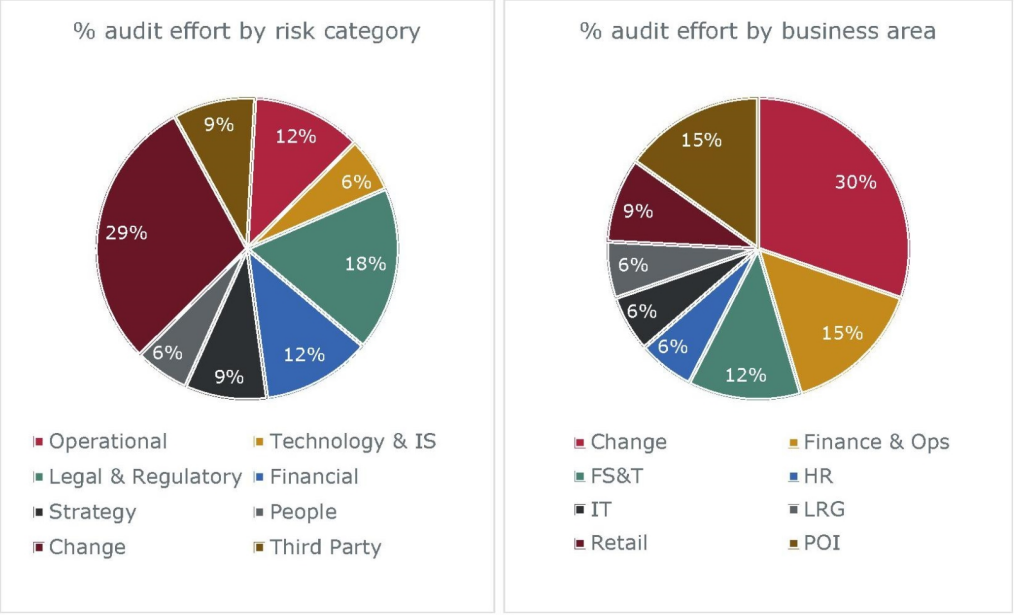
	Topic / Area
1	Oversight of Third Parties
2	Senior Managers & Certification Regime (SMCR)
3	Pricing: Principles, policies and process
4	Nemesis Project (Programme assurance)
5	MI Platform

Resource Requirements

16. The approved headcount for the internal audit team is 5 FTEs. We are currently at full headcount. The co-source requirement to support delivery of the 2019/20 plan was estimated at approximately 467 days with a total cost of £506k.

Audit Coverage & Benchmarking

17. The proposed plans for POL and POI will jointly provide coverage of all principal risk categories and across all business areas as illustrated below:



18. We have benchmarked Post Office internal audit cost against Deloitte's 2018 Global Auditing Information Network (GAIN) Survey. The table below indicates that Post Office's spend on internal audit services is comparable with similar size FS organisations and higher than similar size retail organisations. It should be noted, however, that the cost of Post Office internal audit would be inflated by the higher London wage costs and the more expensive co-source element of the function.

POL00423454

GAIN industry group	GAIN survey grouping (revenues)	Average gross revenue across group ($)	Average IA costs ($)	Average IA costs as % of revenue
Financial Services / Banking / Insurance (135 respondents)	$500m - $1bn	586,810,000	2,038,190	0.35%
	$1bn - $5bn	1,583,230,000	1,853,290	0.12%
Retail (29 respondents)	$500m - $1bn	726,925,000	310,602	0.04%
	$1bn - $5bn	2,015,000,000	852,702	0.04%
Post Office comparison (FX rate of £1 = $1.31)		**$1,253,670,000**	**$1,763,260**	**0.14%**
		£957,000,000	**£1,346,000**	**0.14%**

Three Year Rotation Plan

19. In 2017/18 we introduced a rotational audit plan to assess core business processes over a three year cycle to provide regular assurance on the effective operation of controls over critical business processes. The rotational plan in the table below has been based on the last review of these processes, known issues and ongoing remedial programmes.

Core Processes – 3 Year Rotation Plan		
Year 1: 2017/18	**Year 2: 2018/19**	**Year 3: 2019/20 (in plan)**
Financial Reporting Controls	Financial Reporting Controls	Financial Reporting Controls (CFS controls post BOT)
Sales (Mails Process)	Sales (Postal Orders)	Sales (Savings)
Business Continuity	Payroll	Employee Expenses (follow-up)
IT Operations (IT Gover-nance & Risk management)	Employee Expenses	Regulatory Compliance
Fixed Assets	Financial Close Process [2]	FS Conduct Management
Treasury Operations	Contract Management	Bill to Cash (Accounts Receivable)
	Agents Remuneration	Supply Chain Management [1]
	Client Settlements Process	Procure to Pay [1]
		Branch Cash Forecasting [1]

[1] Postponed from 2018/19 to 2019/20 [2] Brought forward from 2019/20

20. Appendix 2 contains supplementary information to demonstrate the coverage of all Post Office's principal risks to be achieved over a 3 year cycle (2017/18 to 2019/20).

8.2

POL00423454

Appendix 1 – High level audit scope statements

Rank	Proposed Review	High Level Scope
1	Procure to Pay	To assess the operating effectiveness of the Procurement process through to Accounts Payable and the controls in place to ensure compliance with regulation and to prevent fraud. Consider using Deloitte's 'Moneyback Analytics' to test for duplicate payments. In addition the review will include a follow-up of the 2018/19 procurement fraud investigation.
2	Branch Cash Forecasting	This review will consider the system and processes used for Branch Cash Forecasting and Management as well as the fitness for purpose of the outputs. Also the potential to reduce cash holdings in the Network.
3	Supply Chain (CViT)	To review the operating effectiveness and control of the CViT operation within PO. To include the new CWC system (Transtrack) and to ensure compliance with all relevant regulation - industry (SIA) and fleet / vehicle related (VOSA / CPC Compliance etc.).
4	Accounts Receivable	To review the controls, processes and operating effectiveness of the AR function. To include the management and accounting of aged debtors.
5	Agent On-boarding	To review the operating effectiveness of the controls and processes for the recruitment, verification and training of new agents / partners.
6	Pensions Follow-up	To review the processes and controls in place over pensions administration and ensure they are operating effectively and compliantly (follow-up to the 2018 audit).
7	Employee Expenses Follow-up	To review the processes and controls in place and ensure they are operating effectively and compliantly - with particular emphasis on the evidencing and authorisation of claims - as a follow up to the 2018 audit. Controls over Corporate Credit Cards to be in scope.
8	Branch Banking Framework	To review the maturity of the controls over the Branch Banking Services with focus on operations. Will also follow-up on findings from 2017/18 audit. To include the management of relationships with the partner banks and PO's ability to demonstrate adequate conduct in branches.
9	Sales (Savings Accounts)	Product deep-dive to assess processes and controls around product design, management, monitoring and reporting. To take into account any changes to product (distribution / governance) following the outcome of negotiations with BoI.

POL00423454

10	Vetting / Fit & Proper	To review the processes and controls by which POL ensures its employees conform to internal and external expectations around behaviours including competency and capability. To include vetting of joiners and movers, and activities to monitor continuing fitness and propriety.
11	Effectiveness of Risk Management Framework	To review effectiveness of POL's Risk Management function within the second line of defence. To include assessment of the risk management framework, process and governance, and the extent to which the function supports POL in achieving its strategic and operational objectives.
12	CFS Controls (Post Back Office Transformation programme)	To assess the design and operating effectiveness of the Financial Reporting Controls following the Back Office Transformation programme. The review will focus on controls that changed when processes migrated from POLSAP to CFS.
13	Effectiveness of Compliance Function	To review the operational effectiveness of the compliance function within the second line of defence. To include assessment of the functional scope and reporting touchpoints to allow POL to understand and manage compliance risks as per its stated appetite. To include the financial crime second line activity.
14	Telecoms Customer Billing	To review the processes and controls in place to ensure telecoms customer billing meets regularity requirements, incl. PSD2. To include controls over third party billing systems and reports.
15	Data Privacy (incl. follow-up of GDPR)	Assess the operational effectiveness of the structure, process and controls in place to ensure ongoing GDPR compliance. To follow up the actions from the 2017/18 GDPR programme review to ensure those controls are embedded and sustainable.
16	Cyber Security Follow-up	To assess the implementation of the agreed actions and evaluate the level of progress towards increased Cyber Security Maturity. This will involve periodic (6-monthly) reviews to assess progress made with the areas / domains highlighted by the 2018/19 review to be in most need of improvement.
17	Payzone Control Framework	Assess the design and operating effectiveness of key business and IT controls, as well as the effective operation and reporting of risks and control deficiencies into Payzone Board and into Post Office governance structures. The review will also follow up on the progress to exit TSAs and reverse TSAs that are still in effect, and any deficiencies arising from the Q4 FY18/19 Payzone Acquisition programme review.
18	FS Branch Sales	To assess the design and operating effectiveness of the New Distribution Model to ensure it is compliant with regulation and supports the FS sales strategy.

POL00423454

Appendix 2 – 2017/18 to 2019/20 audits mapped against Post Office principal risks

For 2017/18 and 2018/19 the reference number corresponds to the audits on page 14 and the colour indicates the rating:

= Satisfactory = Needs Improvement = Needs Significant Improvement = Unacceptable = Not Rated = In Progress

Principal Risks			Risk Definition	Audit Coverage		
				Proposed 2019/20	2018/19	2017/18
OPERATIONAL	Operational Risk	Process and Service Delivery	The risk of failed transaction processes or process management that are "externally facing" i.e. provide a service for external customers, including agents, clients.	• Sales – Savings Products • Agent On-boarding	36 41 42 46	2 9 5 8
		Product risk	Failure to successfully design, market, deliver, support and improve our product portfolio in a manner that meets customer needs and delivers desired customer outcomes, may lead to adverse financial and reputational impact.	• Banking Framework • *Alt - MoneyGram Product Risk Review*	28 49	10 8
		Payments (Demand / Regulatory)	The risk that Post Office is unable to manage effectively the payment process. Failure to comply with contract regulation, manage high volume of payments or record incorrect payments may result in a reputation damage and financial loss.	• Procure to Pay		
		Records management	Inadequate or insufficient processes and systems for creating, maintaining, retrieving and disposing of contractual, commercial, legal and intellectual property related documents and records, in line with legal and business policy requirements.	• Data Governance Programme (Change) • Data Privacy (GDPR Follow-up)	37 53	13
	Procure	Procure	Potential for failures in a procurement process resulting in loss, disruption, penalties or reputation damage. Suboptimal management of procurement channels (reduced purchase options), could affect the continuity of the business and expose the business to incur high costs that could reduce margins of profitability.	• Procure to Pay	30	
	Safety	Keep our people, customers & 3rd parties safe	The risk to health and safety of colleagues, contractors, customers and third parties (in the workplace, branches and also affected by business activities e.g. acquisition of a vehicle. Breach of Health and Safety regulations).	• Supply Chain (CViT)		

POL00423454

Principal Risks			Risk Definition	Audit Coverage		
				Proposed 2019/20	2018/19	2017/18
		Physically secure	Failure to ensure the physical safety of employees and agents in response to incidents such as theft, robbery, burglary, terrorism and site safety, could expose Post Office to significant costs for reimbursement for damages and remediation, operational disruption and reputational damage.	• Supply Chain (CViT)		
	BCP (excluding ITDR)	BCP (excluding ITDR)	The risk or instances of interruptions (including critical sites, critical and core infrastructure, suppliers and colleagues), as a consequence of internal or external events due to a lack of defined, tested and effective continuity plans and recovery strategies, which may lead to financial, operational and reputational damage.	• *Alt – BCP (follow up)*		12
	Reputation (Brand Protection)	Brand	The risk of losing the trusted brand image of Post Office that prevents the business from successfully operating in its chosen markets and/or achieving its North Star ambitions. The organisation may lose market share, key resources or its ability to compete because of the perception of its behaviour with customers, agents, suppliers and partners.		36	9
	Customer Risk	Customer Risk	The risk that business operations do not meet customer expectations due to a reduced focus on their satisfaction (e.g. vulnerable customers).			9
INFROMATION SECURITY	**IT Security**	IT Security	Inadequate procedures around the management of IT security resulting in cyber threat (denial of service, theft/unauthorised disclosure of valuable information) and insider threat (theft/unauthorised disclosure of valuable information, accidental disclosure, and illegal software use), and leading to financial loss, service disruption and reputational damage.	• Cyber Security Maturity (ongoing re-assessment) • *Alt – Effectiveness of IT Security 2nd line* • *Alt – ID & Access management follow-up*	37	6 7

POL00423454

Principal Risks			Risk Definition	Audit Coverage		
				Proposed 2019/20	2018/19	2017/18
TECHNOLOGY	**Business Interruption (ITDR)**	Business Interruption (ITDR)	The risk or instances of interruptions to IT infrastructure and systems (including at IT suppliers) as a consequence of internal or external events and due to inadequate recovery strategies and/or continuity of systems and controls.	• Belfast Exit (Change)	38	
TECHNOLOGY	**Technology Ops**	Technology Ops	Inappropriate, inadequate or unavailable technological infrastructure (e.g. HW, SW) to support current and future business needs in an efficient and effective way.	• Belfast Exit (Change)	38 46	4 16 26 24
THIRD PARTY	**Dependence on 3rd Parties and Contract manage-ment**	Dependence on 3rd Parties and contract management	The risk that Post Office is unable to effectively manage: - dependency on 3rd parties to deliver, support and improve services for which they have been contracted to the required time, cost or quality; and - its contracts, including failure to negotiate the favourable commercial terms and conditions in contracts, ensuring compliance with the terms and conditions, documenting and agreeing any changes or amendments that may arise during its implementation or execution, which may have an impact on financial and operational performance.	• Telecoms Customer Billing • *Alt - Contract Management, incl. Revenue Contracts (POCA)* • Banking Framework • Agent On-boarding	33 41 53	16 10 8
LEGAL & REGULATORY	**Financial Crime**	Managing losses & fraud	The risk of acts that create financial loss, and/or are intended to defraud, misappropriate property or circumvent the law.		30 35	
LEGAL & REGULATORY	**Financial Crime**	Financial Crime	The risk of financial crime (money laundering, terrorist financing, bribery and corruption, fraud, etc.) resulting from inadequate or failed internal processes, people and systems, or from external events, leading to regulatory breaches and and/or reputational damage to the Post Office; and financial and commercial loss to the Post Office and its customers, colleagues and clients.	• Employee Expenses (follow up) • Vetting / fit & proper • Effectiveness of the Compliance Function	28 29 32 34 40	10
LEGAL & REGULATORY	**Information Protection & Regulatory Compliance**	Data Security	Inadequate procedures around the management of information and its security results in a breach of valuable information (customer, colleague, commercial and/or operational) leading to financial loss and reputational damage.	• Data Privacy (GDPR follow up)	37 49	13

POL00423454

Principal Risks			Risk Definition	Audit Coverage		
				Proposed 2019/20	2018/19	2017/18
		Compliance with laws and regulations	The risk that Post Office faces exposure to losses, penalties and/or reputation damage when it fails to act in accordance with legal and regulatory obligations.	• Effectiveness of the Compliance Function • Vetting / fit and proper • FS Branch Sales	32, 36	1, 13, 14
	Litigation	Litigation	The risk that legal action will be taken because of an individual's or organisation's actions, inaction, products, services or other events. Managers and employees, individually or in collusion, commit illegal acts, exposing the organisation, the management itself and the employees to their consequences.		34	
	Record and pay taxes/VAT	Record and pay taxes/VAT	The risk that the administration of tax/VAT may be more costly - or otherwise more burdensome than foreseen. The risk may arise from existing tax/VAT laws and practice, or from changes in tax/VAT laws and practice.			1
	Governance	Governance	The risk that Post Office organisational infrastructure fails to provide robust oversight of decision making and the control mechanisms to ensure strategies and management instructions are implemented effectively.	• Effectiveness of the Risk Management Framework	34, 48	
	Conduct Risk	Conduct Risk	The risk of customer detriment or censure and/or a reduction in earnings/value, through financial or reputational loss, from inappropriate or poor customer treatment or business conduct.	• Vetting / fit and proper • FS Branch Sales	36, 27	9
FINANCIAL	**Financial Risk**	Reporting results, providing data accurately and effective internal controls	The risk that Post Office suffers reputational damage, loss of shareholder confidence and /or financial loss from the adoption of inappropriate accounting policies, ineffective controls over financial reporting, failure to manage the associated risks in changes to tax, law and failure to disclose accurate and timely information.	• CFS Controls • Payzone Control Framework • Accounts Receivable	31, 35, 39, 43, 47	3, 15, 22, 23
		Sufficient cash / headroom	The risk that Post Office is unable to maintain sufficient cash / headroom for the financial and operational needs of the business.	• Branch Cash Forecasting		

POL00423454

Principal Risks			Risk Definition	Audit Coverage		
				Proposed 2019/20	2018/19	2017/18
		Ensuring sustainable profit	The risk of not securing a sustainable and profitable growth (e.g. not focusing on the long-term performance) could reduce revenue and EBITDAS.		45	
STRATEGY	Strategy Risk	Competitive-ness, Market and Customer Relevance	Failure to develop and implement an effective, coherent and consistent strategy: - aimed at establishing and maintaining a competitive advantage, in response to actions adopted by main competitors, disruptors or new operators; and - in response to changing markets (including demographic, technological and other external market events) and customers changing service needs and expectations.	• Digitising Mails (Change)	49	25 9
		Strategic Risk	The risk that Post office does not have a Strategic Plan or deliver its North Star strategic priorities due to insufficient capability to execute it in line with plans or failure to adapt with agility to respond to changes in the external and internal environment.	• Investment Funding Controls • Benefits Realisation	49	
PEOPLE	Develop, Inspire and Grow	Communicate, inspire and align	Inadequate, inappropriate or ineffective processes relating to recruitment, development, management, reward, engagement and well-being of Post Office employees could result in adverse financial, operational or reputational impact.	• Pensions (Follow-up) • Employee Expenses (Follow-up)	29 34 40	14 17 20 21
CHANGE	Managing change	Managing change	Inadequate and/or inappropriate capabilities, processes, organisation, data and culture to identify, prioritise, design, deliver and manage the portfolio of change activities resulting in delays, cost overruns, and non-realisation of benefits and in turn leading to the business not being able to operate the desire capabilities, processes and systems to support North Star ambitions.	• Benefits Realisation • Effectiveness of Gating Process • Second line Program-me Assurance • In-flight reviews of change programmes (up to 6)	44 45 46 53 49 54	25 17 19 20 26 27 24

"Alt" refers to alternative audit topics from the watch list.

POL00423454

2017/18 Internal Audits Finalised		
1	VAT Process	Needs Improvement
2	Lottery Prize Pay-out	Satisfactory
3	Financial Spreadsheet Controls	Needs Improvement
4	IT Control Framework (Advisory)	Advisory Report
5	Mails Process	Satisfactory
6	Information Security (2016) Follow-up	Needs Significant Improvement
7	IT Security Transformation (Advisory)	Advisory Report
8	Compliance with Banking Framework	Needs Significant Improvement
9	Customer Complaints	Needs Improvement
10	MoneyGram: AML Compliance	Satisfactory
11	Telecoms Control Framework	Needs Improvement
12	Business Continuity	Needs Significant Improvement
13	GDPR Programme	Needs Improvement
14	Pension Scheme(s)	Needs Significant Improvement
15	Financial Control Framework	Satisfactory
16	IT Governance and IT Risk management	Needs Improvement
17	*SAP SuccessFactors - Payroll*	*Needs Improvement*
18	*Integrated Change Plan (Advisory)*	*Advisory Report*
19	*IT Networks*	*Needs Improvement*
20	*SAP SF Payroll Go-Live Readiness Review*	*Acceptable (PwC)*
21	*SAP SF Payroll Lessons Learnt*	*Not Rated*
22	*Back Office Transition Lessons Learnt*	*Not Rated*
23	*Back Office Transformation*	*Not Rated*
24	*Project Solar - HNGT Lite*	*Needs Significant Improvement*
25	*Network Transformation*	*Satisfactory*
26	*Branch Technology - EUC Transition*	*Needs Improvement*
27	*EUM*	*Needs Improvement*

2018/19 Internal Audits Finalised / In Progress		
28	Postal Orders (Product Risk Review)	Needs Improvement
29	Employee Expenses	Unacceptable
30	Procurement Fraud Investigation	Not Rated
31	Month-end Close Process	Satisfactory
32	MoneyGram AML Compliance	Satisfactory
33	Contract Management (IT)	In Progress
34	Whistle-blower Process	Satisfactory
35	Bank Accounts Governance	Satisfactory
36	FS Training & Competence	In Progress
37	Cyber Security	In Progress
38	IT Control Framework	In Progress
39	Financial Control Framework	In Progress
40	Payroll	In Progress
41	Client Settlements (Interim Controls)	In Progress
42	Agents Remuneration	In Progress
43	Network and SGEI Reporting	In Progress
44	*Change Excellence (Trafalgar)*	*Advisory Report*
45	*DMB Strategy*	*Satisfactory*
46	*Branch Hub (Agents Portal)*	*Needs Improvement*
47	*Investment Funding Controls*	*Needs Improvement*
48	*Payzone Integration (Panther)*	*In Progress*
49	*Digital Identity Services*	*In Progress*
50	*Digitising Mails*	*Being assessed*
51	*Payment Technology Upgrade (PCI)*	*Being assessed*
52	*Mails Strategy*	*Being assessed*
53	*Belfast Exit (Migration to Azure Cloud)*	*In Progress*
54	*'One Best Way' Deployment*	*In Progress*

Items in italic print denote Change Assurance reviews

POL00423454

Treasury Risk Management Framework, Policies and Authorities

Author: Mark Dixon Sponsor: Alisdair Cameron Meeting date: 25 March 2019

Executive Summary

Context

The Audit, Risk and Compliance Committee approved the most recent Treasury Risk Management Framework, Policies and Authorities (the "Treasury Policy") at its meeting in March 2018.

Our control framework requires an annual review and update of this document.

This paper provides an update as at March 2019 (the "March 2019 Treasury Policy Update").

Question addressed in this report

1. What changes have been made to the Treasury Policy?
2. How effective has the policy been over the last year in managing the risks it addresses?

Conclusion

The Treasury Framework, Policies and Authorities set out in the Appendix to this report are appropriate for an organisation of POL's size and complexity.

Input Received

The Risk & Compliance Committee reviewed the changes and recommended the approval of the changes and adoption of the revised Treasury Policy at a Committee meeting on 14 March 2019.

Input Sought

The Audit, Risk and Compliance Committee is asked to approve the changes to the Treasury Risk Management Framework, Policies and Authorities set out in this paper.

POL00423454

The Report

What changes have been made to the Treasury Policy?

1. The full Treasury Risk Management Framework, Policies and Authorities are set out in a Schedule to this paper.

2. The main changes proposed in March 2019 from March 2018 are listed below. In March 2018 we concluded a major rewrite of the Treasury Policy. The changes required for the March 2019 Update are therefore considered to be minor.

3. Authorities are delegated to the Chief Financial and Operating Officer (the "CFOO"), the POL Finance Director (the "POL FD"), and the Head of Treasury, Tax and Insurance (the "HoTTI"), being the roles and titles existing as at February 2019. The document has been updated to ensure that where titles change over time authorities will rest with those persons performing substantially the same roles. In any case of doubt confirmation will be provided by the Company Secretary. (See **1 Introduction**.)

4. Drawdowns under facilities require approvals each time a drawdown is made. The delegated authorities vary according to the drawdown period. The delegated authorities for drawing under Other External Borrowings (up to £50m) have been amended to ensure that drawings under the £50m BEIS Short-term Facility can be made quickly and efficiently within deadlines. (See **3 Short-term Cash and Liquidity Management**.)

5. Subsidiaries may have surplus cash balances that they wish to deposit with POL or may have short-term funding needs which can be satisfied by POL. The policy has been redrafted to ensure flexibility for new subsidiaries, including Payzone Bill Payments Limited, and to ensure that intra-group borrowing and lending is still permitted after the completion of Project LEO, provided that such borrowing and lending is permitted under the BEIS Facility and the entity's Articles of Association. The policy delegates authority to the CFOO to agree and execute loans of up to 3 months and £20m on behalf of POL. (See **3 Short-term Cash and Liquidity Management**.)

6. From time-to-time POL may enter into short-term funding arrangements with First Rate Exchange Services Limited ("FRES") under which FRES provides a loan to POL to fund additional holdings of foreign currency note inventory. The policy has been updated to ensure that such loans are permitted and must be executed within the delegated authorities set out in the policy. (See **3 Short-term Cash and Liquidity Management**.)

POL00423454

7. Sections 5 and 6 have been updated to reflect changes to credit ratings over the last 12 months. (See **5 Counterparty Credit Risk Management** and **6 Investment Risk Management**.)

8. As per 5. above the section on Guarantees/Group Support has been rewritten to ensure flexibility for new subsidiaries, including Payzone Bill payments Limited. (See **13 Guarantees / Group Support**.)

How effective has the policy been over the last year in managing the risks it addresses?

9. The Treasury Policy requires that any breaches are reporting to the Operations Board (Treasury Committee) through the monthly Treasury Report. It requires that breaches are immediately reported to the CFOO and the Group Director of Legal, Risk & Governance and, when considered appropriate, at the discretion of the CFOO, to the RCC and ARC.

10. On a number of occasions during the year the closing cash positions were outside the targeted ranges set out in the policy. Each of these occurrences were described in the Treasury Report. The low frequency of such occurrences suggests there is no systemic problem in this area. On three occasions our bank accounts were overdrawn overnight beyond our agreed overdraft limit with Barclays Bank of £5 million. The overdrawn amounts were £5.5 million, £19 million and £17.5 million on 5 June, 11 June and 15 October respectively. Each was described in the Treasury Report. All occurrences were due to late receipts in respect of wholesale note sales. Barclays are notified in advance when we expect to exceed limits; an interest claim is made against the wholesale customer making the late payment; and a discussion had with the customer to reinforce the importance of timely payments. We do not consider any further action to be appropriate.

11. On two occasions during the year we exceeded approved counterparty limits. Both were with Barclays, our cash management bank, for whom we have an agreed limit of £80 million, and on each occasion the breach was no more than £5 million and was for no longer than one night.

    (i) The CFOO was notified, on 17 April 2018, of a breach in our counterparty limit with Barclays Bank overnight. The bank account closed on 16 April with a balance of £83.7m, £3.7m above our £80m limit. The limit breach arose due to failure of CHAPS payments to clients because of Barclays' system problems. The payments were processed on 17 April.

POL00423454

(ii) The CFOO was notified, on 4 January 2019, of a breach in our counterparty limit with Barclays Bank overnight. The bank account closed on 3 January with a balance of £84.3m, £4.3m above our £80m limit. The limit breach arose due to partial failure of CHAPS payments to clients because of an incomplete file reaching Barclays. The payments were processed on 4 January. We have made changes to the approval process to ensure that this is not repeated.

POL00423454

Schedule – Treasury Risk Management Framework, Policies and Authorities - March 2019

Strictly Confidential

POL00423454

POST OFFICE LIMITED AND SUBSIDIARIES (THE "GROUP")

TREASURY RISK MANAGEMENT FRAMEWORK, POLICIES AND AUTHORITIES - MARCH 2019

		Page
I - Introduction		
1	Background	2
2	Policy Overview	3
II - Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity		
Key Policies		
3	Short-Term Cash and Liquidity Management	5
4	Medium and Long-term Funding Management	8
5	Counterparty Credit Risk Management	10
6	Investment Risk Management	12
7	Foreign Exchange Exposure Management	16
8	Interest Rate Exposure Management	18
9	Bank Relationship Management	19
10	Commodity Price Exposure Management	20
Other Guidelines		
11	Operational Banking	21
12	Payments	23
13	Guarantees and Indemnities / Group Support	25
14	Regulatory Obligations	26
15	ISDA Agreements	27
III - Governance and Reporting		
16	Treasury Governance and Reporting	28
APPENDICES		
A	Summary of Counterparty Relationships, Services and Exposures	30
B	CHAPS Banks	31
C	Delegated Authorities for Authorisation Panels	32
D	Delegated Authorities for Drawdowns under Credit Facilities	33
E	Individual Write-off Authority Levels	34
F	Summary of Delegated Authorities	35

POL00423454

I - Introduction

1. Background

1.1. This document sets out the risk management framework, policies and authorities adopted by Post Office Limited ("POL") and its subsidiaries (together the "Group") in relation to its treasury activities and is an update of the paper approved by the ARC Committee in March 2018. It is recognised that Post Office Management Services Limited ("POMS") is subject to regulatory and fiduciary obligations which require derogation from some of the following policies. POMS will determine where there is a conflict between its obligations and these policies and amendments will be agreed and documented. A service agreement will set out the treasury activities which will be carried out on behalf of POMS.

1.2 This document should be read in conjunction with the wider Group Delegated Authorities. For the avoidance of doubt, in the case of inconsistencies the Group Delegated Authorities will prevail.

1.3 The treasury risk management framework has been designed to:

- protect financial asset values;
- minimise income statement volatility;
- ensure financial obligations are met as they fall due;
- secure long-term funding to meet overall business objectives and shareholder return requirements;
- ensure regulatory obligations are met.

1.4 The key treasury risks are:

- *Short-term cash and liquidity risk* – the Group does not have sufficient short-term liquidity to meet payment obligations;
- *Medium and long-term funding risk* – the Group does not have sufficient committed long-term funding in place to meet business objectives and going concern obligations;
- *Counterparty credit risk* – a financial institution counterparty cannot meet its obligations to the Group. Such obligations may arise from: investing the Group's surplus cash balances (see investment risk, below); entering into derivatives transactions; entering into committed facility arrangements; and certain other commercial arrangements with clients.
- *Investment risk* – arising from investing the Group's surplus cash balances;
- *Foreign exchange risk* - arising from holding currency note inventory in branches and cash centres to meet on-demand requirements from customers;
- *Interest rate risk* – arising from the impact of changes in interest rates on the cost of funding, the returns earned on the investment of surplus cash, and the returns earned on the POca cash balances;
- *Bank relationship risk* – the Group does not manage its bank relationships in an appropriate manner;
- *Commodity price risk* – arising from the impact of changes in commodity prices on operational costs;
- *Settlement risk* – the risk that operational and business payments are not executed in accordance with agreed policies and procedures, are not settled in a timely manner or are exposed to the possibility of fraud;
- *Regulatory risk* – arising from POL failing to meet its regulatory obligations around its treasury activities;
- Proper recording of treasury transactions, including the reconciliation of bank statement balances to ledger balances in a timely manner;
- Loss or theft of cash.

1.5 In this document authorities have been delegated to the Chief Financial and Operating Officer (the "CFOO"), the POL Finance Director (the "POL FD"), and the Head of Treasury, Tax and Insurance (the "HoTTI"), being the roles and titles existing as at February 2019. Where titles change over time authorities will rest with those persons performing substantially the same roles. In any case of doubt confirmation will be provided by the Company Secretary.

POL00423454

2. Policy Overview

2.1 The Board is averse to treasury risk. The risk management framework and policies have been designed to reduce risk and concentrate on five principal areas to achieve this:

- **Market Risk**: to minimise any potential loss due to a change in market factors (e.g. interest rates, exchange rates or commodity prices);
- **Credit Risk**: to minimise any potential loss due to a change in the credit-worthiness of a counterparty;
- **Business Risk**: to minimise any potential loss due to economic factors;
- **Operational Risk**: to minimise any potential loss due to system, people, legal and other external events;
- **Regulatory Risk**: to minimise the risk that POL fails to meet its regulatory obligations around treasury activities.

2.2 Day-to-day operation of treasury policy and the activities of the Treasury function are the responsibility of the HoTTI, who reports to the POL FD. Treasury activities are reported on a monthly basis to the Treasury Committee, which is part of the Operations Board, for review and oversight. The composition and responsibilities of the Treasury Committee are set out in section 16.1.

2.3 Any proposed amendments to, or derogations from, policy will be considered in the Treasury Committee and approved by the Audit, Risk and Compliance ("ARC") Committee or, if appropriate, by the Board.

2.4 Treasury is responsible for the following activities. These activities will only be undertaken by Treasury unless an alternative arrangement has been formally approved by the ARC Committee or the Board:

- management of bank account structures to provide automated concentration of cash and/or offset of balances;
- management of the Group's short-term cash flow forecasting process;
- arrangement and management of short-term committed funding;
- monitoring the debt capital structure to ensure that the Group has sufficient funding to support medium and long-term forecast requirements and to minimise refinancing risks;
- management of short, medium and long-term borrowing requirements;
- providing input to and critical review of the Group's medium and long-term cash flow forecasting process;
- fulfilment of obligations under the rules of the Bank of England's Note Circulation Scheme;
- setting counterparty limits for the financial institutions with which Group does business;
- short-term liquidity management and the investment of surplus cash balances;
- executing FX hedges in accordance with the instructions of the FX Committee, using approved instruments to hedge out to a maximum of 6 weeks;
- monitoring net interest rate exposure;
- managing bank relationships, in relation to corporate treasury activity;
- monitoring exposure to commodity price volatility;
- executing payments and administrating payments systems;
- acting as a centre of excellence in providing guidance and advice on all operational banking, payments and other treasury-related matters;
- regularly reviewing mandates;
- ensuring adherence to internal controls around internet banking systems and security;
- ensuring adherence to treasury-related regulatory obligations.

2.5 Cash forecasting must be completed in accordance with Treasury's instructions and deadlines and will support short-term, medium-term and long-term forecasting with the current Strategic Plan of the Board (currently the 5-year plan to 2020/21). Any material variances are to be escalated to the POL FD.

2.6 Compliance with the treasury policies set out in this document is mandatory, subject to the derogations provided to POMS noted in 1.1 above.

POL00423454

2.7 **Delegated Authorities**

- *Approve treasury risk management framework, policies and authorities* - **ARC**
- *Approve amendments to or derogations from Treasury Risk Management Framework, Policies and Authorities* - **ARC**

POL00423454

II Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity

Key Policies

3. Short-Term Cash and Liquidity Management

Business Context

3.1 On a daily basis the Group has significant operating, investing and financing cash flows across its bank accounts, arising in relation to client-related activity across our counters, and as well as its own business-related activity. Client-related inflows and outflows are material and volatile with approx. £65 billion of flows each year. Flows can vary significantly depending on the day of the week and time of year and can also be materially impacted by other factors, out of the Group's control, such as the weather. Even with appropriate long-term committed funding in place there is therefore a short-term liquidity risk that the Group does not have resources available to meet its day-to-day payment obligations as they fall due.

Risk Management Objectives

3.2 The objective of the short-term cash and liquidity management policy is to ensure that the Group has appropriate liquidity in the right place at the right time to meet its payment obligations as they fall due.

Main Policy Statement

3.3 Through a combination of efficient bank account structures and accurate short-term cash flow forecasting, together with access to appropriate levels of committed short-term liquidity, Treasury will ensure that the Group can meet its obligations as they fall due.

Supporting Policy Guidelines

3.4 Bank Account Structures

3.4.1 Where possible, Treasury will manage cash balances within pooling arrangements which enable cash to be efficiently and effectively concentrated and debit and credit balances to be offset. Business units are not permitted to operate bank accounts that are outside these pooling arrangements unless authorised in writing by Treasury.

9.1

3.4.2 **Delegated Authorities**

- *Approve addition of bank account to existing pooling arrangement* - **HoTTI**
- *Approve removal of bank account from existing pooling arrangement* - **HoTTI**
- *Approve creation of new pooling arrangement* - **POL FD**

3.5 Short-term Cash Flow Forecasting

3.5.1 Short-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its day-to-day payment obligations.

3.5.2 Treasury will prepare a short-term, daily rolling forecast of the utilisation of the BEIS Facility and the NRF. The forecast, by day, covers a period of up to two accounting periods. Treasury will issue:

- daily reporting to the HoTTI analysing variances of same-day and two-day forecasts to actuals;
- a weekly Liquidity Report to the CFOO and POL FD updating the forecast for the following week and providing a variance analysis for last week;
- a monthly Forecast Update to the CFOO and POL FD updating the forecast for the following two periods and providing a variance analysis for the last period.

3.5.3 The forecasts and variances will be reviewed on a daily basis by the HoTTI. Monthly

POL00423454

Forecast Updates will be included in the Treasury Report and reviewed by the Treasury Committee. The ARC will be updated by exception.

3.6 Committed Short-term Funding

3.6.1 Treasury's first responsibility is to ensure that sufficient liquidity and facilities are available to the Group to fund its operations. Funding is therefore negotiated and managed centrally and the management of individual cash pools will be dealt with by Treasury.

3.6.2 Short-term liquidity is managed as follows: POL has access to a £950m working capital facility provided by the Department of Business, Energy and Industrial Strategy ("BEIS") (the "BEIS Facility"). The BEIS Facility is available until March 2021. A utilisation request must be provided to BEIS two days before drawdown. Forecasting variances may lead to a shortfall between the amount drawn down and the actual amount required. The strategy to mitigate the risk of a shortfall between forecast and actual funding requirements is to hold a liquid investment reserve of £5m (the "Investment Reserve"). Historically POL has tended to overdraw the BEIS Facility because it did not have access to an emergency source of short-term funding other than the NRF. Any changes to the targeted investment reserve will be reported to the Treasury Committee in the monthly Treasury Report. Treasury can also use a £5m uncommitted overdraft facility with Barclays, use the NRF (see 3.6.3 below), or use the £50m short-term credit facility provided by BEIS (the "BEIS Short-term Facility") (see 3.6.6 below).

3.6.3 In addition, POL is a member of the Bank of England's Note Circulation Scheme (the "NCS"). The scheme allows POL to declare and sell eligible notes to the Bank of England (the "Bank") overnight with a commitment to buy those notes back from the Bank first thing the next morning. This reduces the Group's overnight funding requirement. The NCS rules require the provision of collateral to the Bank. Collateral is currently provided on behalf of POL under a Facilities Agreement entered into by POL with National Westminster Bank Plc[1] under which the bank makes available: a £400m intra-day facility; a £350m overnight NRF facility (for the purposes of providing overnight collateral to the Bank); and, a £1m collateral facility, used in connection with our crime insurance.

3.6.4 The NCS rules also require that POL has a crime insurance in place that is compliant with BoE requirements.

3.6.5 The amount available to be used under the NRF over the course of the Bank's financial year (to October) is constrained by a cap (the "Cap") that POL generates, mainly as a function of outward rems processed from its NCS cash centres. Treasury will monitor utilisation of the NRF against the Cap to ensure that no more than the Cap generated is used over the course of the year and that financial penalties are therefore avoided. Cap generation and NRF utilisation will be reported to the Treasury Committee on a monthly basis via the Treasury Report.

3.6.6 POL has arranged a £50m short-term credit facility with BEIS. The facility is available on a same-day basis up to 11:45 am.

3.6.7 Any new borrowings require Board approval. See 4 Medium and Long-term Funding Requirement.

3.6.8 The delegated authorities for drawdowns are set out in Appendix D and in 3.6.9 below.

3.6.9 **Delegated Authorities**

- *Approve change to Investment Reserve (nil to £20m / for up to 2 weeks)* - **HoTTI**
- *Approve change to Investment Reserve (up to £50m / for more 2 weeks)* - **CFOO**
- *Propose drawdown - under existing credit facilities* - **Dealing Panel**
- *Approve drawdown - under BEIS Facility* - **Various (see Appendix D)**
- *Approve drawdown - under other external borrowings, including the BEIS Short-term Facility (up to £50m)* - **Various (see Appendix D)**

[1] *These facilities were provided by Royal Bank of Scotland plc and were novated to National Westminster Bank Plc in 2018 as part of the restructuring of the bank as a response to the Government's ring-fencing requirements.*

POL00423454

3.7 Short-term Cash & Liquidity Arrangements with Subsidiaries of POL

3.7.1 From time to time subsidiaries[2] of POL may have surplus cash balances which they wish to deposit with POL or they may have short-term funding needs which can be satisfied by POL.

3.7.2 POL is permitted to take loans from or make loans to subsidiaries.

3.7.3 All loans will be documented.

3.7.4 Margins on loans will be agreed between POL and the subsidiary and will be on an arm's length basis.

3.7.5 For short-term loans and deposits up to 3 months, for amounts up to £20m, authority to agree margins and execute documentation, on behalf of POL only, is delegated to the CFOO.

3.7.6 For the avoidance of doubt, any loans to or from a subsidiary will require the approval of the subsidiary's Board.

3.7.7 At March 2019 POL has two subsidiaries: POMS and Payzone Bill Payments Limited. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are subsidiaries under the 2006 Companies Act definition, then 3.7 will also be applicable for loans to/from those subsidiaries.

3.7.8 In 2019 POL is considering a legal entity optimisation project under which certain wholly-owned subsidiaries of POL will become sister companies of POL under a new holding company structure. Provided that loans to/from any sister company are permitted under the BEIS Facility and the entity's Articles of Association then they will be permitted under 3.7 and will be executed within delegated authorities set out herein.

3.7.9 From time-to-time POL may enter into short-term funding arrangements with First Rate Exchange Services Limited ("FRES") under which FRES provides a loan to POL to fund additional holdings of foreign currency note inventory. Such loans are also permitted under 3.7 and must be executed within the delegated authorities set out herein.

3.7.10 **Delegated Authorities**

- *Approve margin on intra-group loans to/from subsidiaries on behalf of POL (up to £20m / up to 3 months)* - **CFOO and Head of Tax**
- *Execute documentation for intra-group loans to/from subsidiaries on behalf of POL (up to £20m and up to 3 months)* - **CFOO**
- *Execute documentation for intra-group loans to/from subsidiaries on behalf of POL (over £20m or over 3 months)* - **POL Board**

[2] *As defined under 2006 Companies Act.*

POL00423454

4. Medium and Long-term Funding Management

Business Context

4.1 The Group develops its strategic objectives and prepares long-term business plans to meet those objectives. Such objectives will include the continued participation in the Bank of England's Note Circulation Scheme (the NCS") in order to ensure an adequate supply of notes for the branch network. The Group must ensure that it has sufficient committed long-term funding in place to meet these plans. There is a risk that the funding in place is not sufficient to achieve business objectives or to adequately withstand unforeseen changes to plans.

4.2 In order to present its financial statements on a going concern basis the Group must demonstrate, on an annual basis at each balance sheet date, that it has sufficient committed funding in place.

4.3 The Group's existing funding arrangements, including the facilities made available to enable participation in the NCS, are set out in 3 Short-term Cash and Liquidity Management.

Risk Management Objective

4.4 The objective of the medium and long-term funding management policy is to ensure that the Group has sufficient committed long-term funding in place to meet business objectives and going concern obligations.

Main Policy Statement

4.5 Through a combination of accurate medium and long-term cash flow forecasts and the monitoring of headroom, together with access to appropriate levels of long-term committed funding, the Group will ensure it has sufficient funding in place to meet business objectives and going concern obligations.

Supporting Policy Guidelines

4.6 Medium and Long-term Cash Flow Forecasting

4.6.1 Medium and long-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its business objectives and loan repayments.

4.6.2 Treasury will provide input to Group's medium and long-term forecasts, in particular the one-year and five-year strategic forecasts and in accordance with the current Board Strategy.

4.7 Funding Strategy

4.7.1 The CFOO and the POL FD will recommend to the Board the appropriate debt capital structure for the Group. The Group will have a debt maturity profile and funding structure adequate to meet its:

- business objectives, including growth strategy;
- going concern obligations.

4.7.2 The debt capital structure and maturity profile will be monitored by the CFOO and POL FD, and reviewed by the Treasury Committee to ensure that the Group has appropriate funding available to support its long-term plans. Where possible, the Group seeks to minimise its refinancing risk by adopting a range of maturities for its debt facilities. Maturity of existing facilities will be monitored to ensure that negotiations commence in a timely manner to extend or replace them.

4.8 Headroom

4.8.1 *Facility Headroom* - Facility Headroom is defined as the headroom available under the BEIS Facility. The Group will aim to maintain Facility Headroom of at least £200m (the "Facility Headroom Buffer"). Any reduction in Facility Headroom Buffer will require Board

POL00423454

approval. It will be monitored and reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.2 *Security Headroom* - Security Headroom is defined in the BEIS Facility. Treasury will also monitor the asset security headroom of the BEIS Facility. It will be reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.3 Treasury will use a combination of the short-term forecasts outlined in 3.5 above and the medium and long-term forecasts to monitor headroom.

4.8.4 **Delegated Authorities**

- Approve amendment to Facility Headroom Buffer - **Board**

4.9 Borrowing Policy

4.9.1 Borrowing is only permitted in sterling unless approved by the ARC.

4.9.2 Borrowing should only be incurred in accordance with the restrictions under clause 10 of POL's Articles of Association and may require shareholder approval.

4.9.3 Additional borrowing is only permitted in accordance with the constraints imposed under the BEIS Facility which limits borrowings as follows:

- the existing £950m BEIS Facility itself, or any refinancing thereof;
- up to £50m of additional finance or capital leases;
- up to £50m additional other borrowings.

Together with the facilities in place to support POL's participation in the NCS, namely:

- the £400m intra-day facility;
- the £350m overnight NRF facility.

4.9.4 **Delegated Authorities**

- Approve new medium and long-term funding - **Board**

POL00423454

5. Counterparty Credit Risk Management

Business Context

5.1 Counterparty credit risk arises where a financial institution counterparty cannot meet its obligations to the Group. Due to the nature of POL's business activities such exposures arise both as part of POL's normal corporate treasury activities and its other client-related activities. Exposures arise primarily as follows:

Corporate Treasury Activity

5.1.1 *Investment of Surplus Cash Balances* - Total exposure of approximately £5m but may increase up to £50m when the investment reserve is increased during holiday periods. (See 6. Investment Risk Management.)

5.1.2 *Mark-to-Market of Derivatives* - Derivative contracts (including FX swaps, FX forwards and interest rate swaps) where the mark-to-market position has moved in favour of POL such that the counterparty owes money to POL under the contract. Exposure arises due to changes in market rates. Because FX maturities are managed within one month total exposure is currently minimal.

5.1.3 *Committed Facilities* - Commitments made by a bank or other funding provider under facilities that remain undrawn by POL. Such facilities currently comprise: the BEIS Facility and the BEIS Short-term Facility; and, the £400m intra-day facility / £350m overnight NRF facility provided by National Westminster Bank Plc. The exposure relating to the BEIS Facility and the BEIS Short-term Facility is considered to be nil but there is an exposure on National Westminster Bank Plc that fluctuates during the day depending on how much is utilised under the facilities. Total exposure may be up to **£400m**.

Other Client-Related Activity

5.1.4 *Banking Framework* - Over-the-counter banking transaction services with retail and business customers. Transactions are cleared through the LINK system with daily settlement to POL received from Barclays Bank PLC this creates a daily net direct exposure to Barclays Bank PLC of up to **£30m**. In addition, POL would also be exposed to the failure of an individual client bank to meet its obligations under the LINK system.

5.1.5 *Debit and Credit Card Processing* - When a customer makes a payment to POL over-the-counter using either a debit card or a credit card settlement is received by POL via GPUK LLP ("GlobalPay") on the next business day. This creates a one-day credit exposure against GlobalPay. Total exposure fluctuates but is approximately **£75m**.

5.1.6 *Cheque Clearing* - when a customer makes a payment to POL using a cheque it creates a short-term exposure (up to two days) exposure against the bank on which the cheque is drawn. The total exposure on cheques is approximately **£25m** but this is disaggregated between the banks on which the cheques are drawn.

5.1.7 *Other Client-Related Activity* - Exposures arising from other client-related activities.

- ATM Withdrawals – Exposure to Bank of Ireland linked to cash withdrawals from ATMs. The exposure varies significantly, depending on the time of the year and day of the week, between **£20m** and up to **£135m**.

- POca Related Flows – Exposure to JPMorgan Europe Limited in respect of POca-related flows across POL counters. Flows between 13:00 on the previous day and 13:00 are aggregated and paid same day. The exposure fluctuates significantly depending on the day of the week and time of the year and is impacted by holiday periods and winter fuel payments. It can vary between **£20m** and up to **£125m**.

5.2 This policy focuses on counterparty credit risk arising from POL's corporate treasury activities.

POL00423454

Risk Management Objectives

5.3 The objective of the counterparty credit risk management policy is to minimise the Group's risk of loss in its corporate treasury activities as a result of the failure of a financial institution counterparty.

Main Policy Statement

5.4 Treasury will minimise the risk of loss due to the failure of a financial institution counterparty to meet its obligations by only entering into corporate treasury transactions with highly-rated counterparties and through credit approvals, limits and monitoring procedures.

Supporting Policy Guidelines

5.5 Treasury will only enter into corporate treasury transactions with appropriately approved financial institution counterparties.

5.6 The Group's corporate treasury-related credit risk arises primarily from the investment of surplus cash balances. For the purpose of the investment of surplus cash balances limits are allocated according to rating band rather than specified counterparty. Approved counterparties and sub-limits applicable to deposits (as at March 2019) are set out in 6 Investment Risk Management. Deposit limits will fluctuate with changes to credit ratings.

5.7 When monitoring the credit quality of counterparties Treasury will use short-term and long-term credit ratings from S&P and Fitch. The weaker of the two ratings will be used for decision-making purposes.

5.8 Approved counterparties and credit limits for other transaction types are set out in Appendix A.

5.9 New counterparties and limits may be approved from time to time. Treasury will make a recommendation to the Treasury Committee based on credit ratings for consideration and recommendation to the ARC.

5.10 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report. See 6. Investment Risk Management. Exposures to corporate treasury counterparty activities will be aggregated (including investment counterparties) and reported to the Treasury Committee on a monthly basis together with changes to credit ratings as part of the Treasury Report.

5.11 **Delegated Authorities**

- *Approve new financial institution counterparty* - **ARC**
- *Approve financial institution counterparty limit* - **ARC**
- *Approve temporary increase to financial institution counterparty limit* - **CFOO**

5.12 Note on the Implications of Ring-fencing - *Effective 1 January 2019 the major UK banks were required to implement the Government's ring-fencing requirements. In 2018 the Group's bank accounts and the £400m facilities with Royal Bank of Scotland Plc were transferred to National Westminster Bank Plc as part of the bank's restructuring to meet these requirements. From 2019 these accounts and facilities will sit inside the ring-fence. (It should be noted that the interest rate swap executed in April 2018 with NatWest Markets Plc sits outside the ring-fence.) Provided that the S&P and Fitch long-term and short-term credit ratings of National Westminster Bank Plc (or any other entity inside or outside the ring-fence) were the same as, or better than, Royal Bank of Scotland Plc then all references to Royal Bank of Scotland Plc were deemed to apply to National Westminster Bank Plc (or those other entities). This approach was also applied for Barclays Bank PLC and Lloyds Bank plc.*

POL00423454

6. Investment Risk Management

Business Context

6.1 Treasury manages short-term liquidity to target a cash buffer of £5m. The buffer is reduced to nil at period ends and can be increased up to £50m around holiday periods when liquidity risks are highest. This creates surplus cash balances that can be invested by Treasury.

Risk Management Objectives

6.2 The three core objectives of the Group's investment risk management policy are: (i) *security* – to preserve the principal sum; (ii) *liquidity* – to ensure investments are accessible when needed; (iii) *yield* – to optimise return on investments.

Main Policy Statement

6.3 The Group's overall consideration when depositing surplus cash balances is the preservation of the principal sum. Surplus cash balances will be invested by Treasury to optimise return, subject to counterparty credit risk considerations. These investments will not be subject to fluctuation in capital values.

Supporting Policy Guidelines

6.4 Permitted Investment Instruments - Treasury are permitted to use the following investment instruments: bank term deposits and deposits on interest-bearing accounts; money market funds ("MMFs"); and, when appropriate, deposits with the Debt Management Office ("DMO").

6.5 Permitted Currencies – Treasury will only invest in £-denominated instruments.

6.6 Approved Bank Counterparties and Deposit Limits - It is the Group's policy to establish and monitor limits for each of the counterparties that it makes investments with.

6.6.1 Limits for term deposits and interest-bearing accounts ("deposit limits") are based on credit rating bands rather than specific counterparties. Counterparties are allocated to bands based on the lower of the S&P and Fitch long-term credit rating as follows:

Credit Rating (1)	Approved Limit (£m)
AAA	120
AA+ to AA-	90
A+ to A-	60
BBB+	30
BBB and below	0

(1) Based on lower of S&P and Fitch long-term credit rating

6.6.2 Counterparties must have a long-term S&P or Fitch credit rating of at least BBB+ and a short-term S&P or Fitch credit rating of A2/F2.

6.6.3 Counterparties must also be a member of CHAPS (see Appendix C for a list of CHAPS banks).

9.1

POL00423454

6.6.4 Approved counterparties and deposit limits based on credit ratings as at January 2018 are:

Financial Institution Counterparty	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Approved Deposit Limit (£m)
Barclays Bank PLC	**A**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	80.0
National Westminster Bank Plc (1)	**A-**	**A-2**	**Positive**	**A+**	**F1**	**Negative**	60.0
NatWest Markets Plc (2)	**BBB+**	**A-2**	**Positive**	**A**	**F1**	**Negative**	Not applic.
Lloyds Bank Plc	**A+**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	60.0

(1) Entity inside ring-fence; (2) Entity outside ring-fence.

6.6.5 The deposit limits against individual institutions are expected to change with changes in credit ratings.

6.6.5 *Exception* - Barclays Bank PLC, as our cash management bank, is allocated an additional limit of £20m to allow for cash held as operational balances on bank accounts from time to time. Barclays' long-term rating of A+ would imply a deposit limit of £60m. The limit is increased to £80m.

6.7 Other

6.7.1 Unauthorised arbitrage is prohibited i.e. funds should not be specifically drawn down for investment purposes.

6.7.2 Only Treasury is permitted to invest surplus cash balances.

6.7.3 A proposal for the investment of surplus cash balances will be made by the Dealing Panel and approved by either the Treasury Authorisation Panel (see Appendix C – Delegated Authorities for Approval Panels) or in accordance with 6.11 below.

9.1

6.7 Deposit Tenor Limits

6.7.1 Deposits will be no longer than one month.

6.8 Money Market Fund Investment Criteria - It is the Group's policy to establish and monitor limits for each of the MMFs that it invests in.

6.8.1 The MMF must be rated by at least one of S&P and Fitch. If rated it must be rated AAAm by S&P and AAAmmf by Fitch.

6.8.2 POL's holding as a proportion of the fund size must not be greater than 10%.

6.8.3 MMFs must have a constant net asset value (CNAV) (also referred to as stable NAV) or a Variable Net Asset value (VNAV) (also referred to as accumulating NAV).

6.8.4 MMFs must have daily liquidity.

6.8.5 Investment is limited to £50m in any one MMF.

6.8.6 Investment in Prime Liquidity Funds is limited to £350m.

6.8.7 Investment in Government Funds is limited to £150m.

6.8.9 Where a single provider has segregated Prime Liquidity Funds and Government Funds, investments can be made in both MMFs subject to the limits above.

POL00423454

6.9 Approved MMFs and limits as at January 2018 are:

Name of Fund	Credit Rating S&P	Credit Rating Fitch	Asset Class	Currency	Name of Return	Fund Size (£m)	Approved Limit (£m)	Approved Limit / Fund Size (%)
IGNIS - Sterling Liquidity Fund (Standard Life)	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	14,400	50.0	0.3%
Invesco STIC Global Sterling Liquidity Portfolio	**AAAm**	**AAAmmf**	Prime	GBP	CNAV		50.0	#DIV/0!
Aberdeen Liquidity Fund (Lux) - Sterling Fund	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	14,400	50.0	0.3%
Blackrock - Institutional Sterling Liquidity Fund	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	36,800	50.0	0.1%
Goldman Sachs - Sterling Liquid Reserves Fund	**AAAm**	**na**	Prime	GBP	CNAV	11,800	50.0	0.4%
Unallocated	**AAAm**	**AAAmmf**	Prime	GBP			100.0	
Sub-total - Prime Liquidity Funds							**350.0**	
Blackrock - Institutional Sterling Government Liquidity Fund	**AAAm**	**AAAmmf**	Government	GBP	CNAV	2,400	50.0	2.1%
Unallocated	**AAAm**	**AAAmmf**	Government	GBP			100.0	
Sub-total - Government Funds							**150.0**	

6.10 DMO Investment Criteria – The Group may invest with the DMO on an unlimited basis.

6.11 Operational Approvals - For each individual investment made approval is required as per the table below:

Investment Amount	< £300m	< £100m	< £50m	< £300m	< £50m	< £50m
Term of Investment	< 1 month	< 3 months	< 6 months	< 1 year	< 1 year	< 1 year
Delegated Authority	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*POL FD*	*CFOO and 1 other POL Board Member*	*POL Board*

The POL FD is also authorised to approve investments with a maturity of up to 5 years for the purpose of providing collateral for the Note Circulation Scheme.

9.1

6.12 Monitoring

6.12.1 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report.

6.13 Limit Breaches

6.13.1 When Treasury are aware of a potential breach in advance (for example, when Treasury choose to hold in excess of the authorised limit because no other investments opportunities are available) approval must be obtained from either the CFOO or the POL FD for a temporary increase to the limit. The temporary increase will normally be for no longer than one night.

6.13.2 When Treasury are not aware of the breach in advance (for example, where we receive more cash into our Barclays accounts than we had forecasted) Treasury will notify the CFOO of the breach immediately on becoming aware of it but in any event no later than close of business on the day after the breach occurred.

POL00423454

6.13.3 All limit breaches will be reported to the Treasury Committee in the monthly Treasury Report.

6.14 **Delegated Authorities**

- *Approve new investment counterparty - within approved credit rating bands* - **POL FD**
- *Approve changes to credit rating bands for deposit limits* - **ARC**
- *Approve temporary increase to investment counterparty deposit limit* - **CFOO**
- *Approve new permitted investment instrument* - **CFOO**
- *Propose investment of surplus cash balances* - **Dealing Panel**
- *Approve investment of surplus cash balances* - **Various (see 6.11)**

POL00423454

7 Foreign Exchange Exposure Management

Business Context

7.1 Foreign exchange risk principally arises from holding foreign currency note inventory in branches and cash centres to meet "on demand" requirements from customers. All currencies are purchased from FRES. The exchange risk arises from the time of purchase from FRES to the sale of currency to the customer. The size of balances on hand is determined by demand. POL holds note inventory balances in approximately 70 currencies. On average, currency holdings are c. £60m but can peak at over £100m during holiday periods.

Risk Management Objectives

7.2 The objective of the foreign exchange exposure management policy is to minimise the impact on the Group's income statement of foreign currency exposures arising from its day-to-day operations.

Main Policy Statement

7.3 Through a combination of periodic monitoring of foreign exchange exposures and entering into hedges within approved hedging bands the Group will ensure its exposure to fluctuations in exchange rates is minimised.

Supporting Policy Guidelines

7.4 The Head of Travel Money analyses the report of foreign currency note holdings in the network which is prepared by Supply Chain and the daily reports of foreign currency holdings provided by Treasury.

7.5 A monthly meeting of the FX Committee is held, attended by: the Director of Product; the Finance Director Financial Services and Telecoms; and the Head of Travel. The meeting is held to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy outlined below.

7.6 Detailed foreign exchange risk management policy statements

7.6.1 EUR and USD holdings will be hedged 100%; currencies with exposures over £1.5m will be hedged 90% to 100%; other currencies with exposures over £1 million will be hedged 70%.

7.6.2 At least 80% and no more than 120% of qualifying exposures will be hedged based on the average of (1) the previous period's actual holdings and (2) the forecast for one month forward.

7.6.3 Hedges will be closed out and reset to periods between two weeks and five weeks. Longer-dated hedges will be set to mature at a monthend and will be revalued at each intervening month end based upon the mark-to-market valuation provided by the hedging bank.

7.6.4 Hedging will be conducted with counterparties approved by the Treasury Committee (see 5 Counterparty Credit Risk Management).

7.6.5 Trades will be executed at a pre-arranged margin with all counterparties.

7.6.6 The maturity of financial instruments used to hedge foreign exchange exposures will normally be about a month but can be no longer than six weeks.

7.6.7 Permitted Instruments - Foreign currency exposures can only be hedged using foreign currency outright forwards or swaps.

7.6.8 FX hedging instruments can only be used to hedge exposures generated by holding currencies to meet on-demand transactions by customers.

POL00423454

7.7 Latest currency holdings and hedges will be reviewed at the end of each period immediately before the maturity of the monthly hedges by Financial Director Financial Services and Telecoms and the Head of POL Travel.

7.8 On a monthly basis the Finance Director Financial Services and Telecoms will report to the Treasury Committee on the gain or loss on foreign currency holdings.

7.9 From time-to-time POL may enter into short-term funding arrangements with First Rate Exchange Services Limited ("FRES") under which FRES provides a loan to POL to fund additional holdings of foreign currency note inventory. For permissions and authorities in connection with such loans see 3.7.9.

7.10 Any proposed changes to the policies above will be presented to the ARC Committee for approval.

7.11 **Delegated Authorities**

- *Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee* - **Treasury**
- *Approve new permitted FX hedging instrument* - **CFOO**
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – up to £50m* - **CFOO**
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – above £50m* - **Board**

POL00423454

8 Interest Rate Exposure Management

Business Context

8.1 The Group is exposed to changes in interest rates via its Libor-linked funding and the returns it earns on cash balances. Increases in interest rates will increase the Group's cost of funding and increase the return it earns on cash, mainly linked to Post Office card account ("POca") balances.

8.2 The Group's funding is via the BEIS Facility maturing in 2021 and the NRF. Interest rates on both facilities are linked to Libor. POL also earns commission (credited to revenue) on the balances of benefit payments held by JP Morgan, the POca cash balances. The commission interest received is also linked to Libor. The interest receivable on the POca cash balances has historically exceeded the interest payable on POL's borrowings and is expected to do so for the foreseeable future, despite the long-term decline of POca cash balances. The interest payable on POL's funding is a natural hedge of the commission interest receivable.

Risk Management Objectives

8.3 The objective of the interest rate risk management policy is to minimise exposures to income statement impacts of changes in interest rates.

Main Policy Statement

8.4 The Group will monitor its exposures to changes in interest rates on a regular basis and recommend hedging strategies, if appropriate.

Supporting Policy Guidelines

8.5 Treasury will obtain forecasts of interest payable / commission receivable and the net interest rate exposure will be monitored by Treasury and, if appropriate, a proposal to hedge the exposure will be put to the Treasury Committee prior to approval by the Board.

8.6 The suitability and effectiveness of the interest rate risk management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

8.7 Permitted Instruments - Hedging will be by way of interest rate swaps. Other instruments may be approved by the ARC on a case-by-case basis.

8.8 The Government's Managing Public Money Guidelines allow organisations to consider the use of derivatives but require them to consider their use carefully especially to assess value for money. The Guidelines require POL to consult its sponsoring department / HM Treasury before executing any derivative for the first time.

8.9 **Delegated Authorities**

- *Approve new permitted interest rate hedging instrument* - **ARC**
- *Approve execution of interest rate hedging strategy* - **Board**

POL00423454

9. Bank Relationship Management

Business Context

9.1 Good long-term relationships with banks are crucial to the success of the Group around its corporate treasury activities. The Group requires support from banks across all its treasury activities and this support is particularly important for the provision of: short-term liquidity, including operational overdrafts; credit facilities to enable continued participation in the Note Circulation Scheme; and, FX instruments and other derivatives, requiring credit to be extended.

9.2 Due to the UK-focused nature of the Group, the limited requirement for external funding and a small amount of ancillary treasury business, the Group has historically focussed on building relationships with a small group of UK clearing banks.

Risk Management Objective

9.3 The objective of the bank relationship management policy is to establish, maintain and develop efficient and effective banking relationships with a core group of banks to provide the Group with long-term banking support irrespective of short-term business conditions and financial market turbulence.

Main Policy Statement

9.4 The Group will seek to build long-term relationships with two to three of the UK clearing banks.

Supporting Policy Guidelines

9.5 It is the Group's policy to build long-term relationships with providers of banking services and facilities in order to maximise mutual advantage. In allocating new business opportunities, preference will generally be given to banks where a relationship already exists, but this does not preclude the use of other banks identified by Treasury should it be appropriate. Any new relationships will be reported to the Treasury Committee in the monthly Treasury Report for approval.

9.6 Current counterparty relationships, including banks, are listed in Appendix B.

9.7 Management of the Group's bank relationships is the responsibility of the HoTTI and the Chief Financial and Operations Officer ("CFOO"). Bank selection will be determined by a number of factors, including service, price, product range, geographic spread and willingness to provide services. The decision to develop a new relationship will rest with the Treasury Committee.

9.8 From time to time POL may require that banking partners enter into Non-Disclosure Agreements ("NDAs") to protect Group-sensitive information. Approval will be required by the CFOO.

9.9 **Delegated Authorities**

- *Approve entering into relationship with new bank* - **Treasury Committee**
- *Approve entering into relationship with new bank (prior to Treasury Committee approval)* - **CFOO**
- *Approve entering into NDA with bank* - **CFOO**

POL00423454

10 Commodity Price Exposure Management

Business Context

10.1 The Group is exposed to movements in the price of diesel, gas and electricity used throughout the business.

Risk Management Objectives

10.2 The objective of the commodity price exposure management policy is to minimise income statement volatility due to changes in commodity prices.

Main Policy Statement

10.3 Treasury will monitor exposures to these commodities and forecast price movements and may recommend hedging action to the Treasury Committee or directly to the CFOO to protect the Group from adverse price movements.

Supporting Policy Guidelines

10.4 The CFOO is authorised to hedge each commodity, where it is believed to be economic to do so, up to a maximum of 3 years based on forecast future usage.

10.5 Permitted Instruments - permitted hedging instruments are spot purchases, currency deposits, forward contracts, call options, matched options (e.g. cylinders) and swaps. Futures will not be used without specific authority of the CFOO.

10.6 The Group will designate commodity cash flow hedges against forecast underlying exposures. Unrealised gains and losses on hedges will be deferred in reserves. This will be recycled to the income statement when the hedge matures to match forecast expenditure.

10.7 The suitability and effectiveness of the commodity price exposure management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

10.8 **Delegated Authorities**

- *Execute commodity price hedges within policy* - **Treasury**
- *Approve new commodity price hedge counterparty* - **CFOO**
- *Approve execution of commodity price hedge within policy* - **HoTTI**

POL00423454

Other Guidelines

11. Operational Banking

11.1 Bank Facilities

11.1.1 Treasury is responsible for the negotiation of all operational banking facilities and any changes to existing operational facilities. Such facilities include overdrafts, fx lines, BACS limits, intra-day limits and any similar arrangements. Directorates do not have the authority to negotiate or commit to any new operational banking facilities without prior approval from Treasury and are not authorised to undertake any discussions regarding credit lines.

11.1.2 All changes to existing operational banking facilities or any new operational banking facilities must be agreed by the CFOO.

11.2 Interest and Bank Charges

11.2.1 Bank transaction charges will be negotiated by Treasury to ensure minimum cost to the Group. Charges incurred will be reviewed by Treasury to ensure that the activity levels and unit costs applied by the banks to calculate charges are in accordance with agreed tariffs. Errors are to be notified directly to the bank.

11.3 Bank Accounts

11.3.1 It is the Group's policy to minimise the number of bank accounts it operates. Treasury will conduct a bi-annual audit to ensure it has an accurate record of bank accounts. Accounts not being utilised should be closed. This will be reconciled back to internal and bank records.

11.3.2 All new bank accounts will be approved by the HoTTI.

11.3.3 Where possible all accounts should be within a cash pooling arrangement. It is recognised that certain constraints apply to POMS cash, where restrictions may preclude pooling.

11.4 Bank Mandates

11.4.1 It is the Group's policy to standardise bank mandates wherever possible. Treasury will manage and administer all bank mandates centrally. Each bank account must be supported by a written, up-to-date mandate which is checked against a list of those colleagues leaving the business on a monthly basis.

11.4.2 Authority levels relating to internet banking systems will be documented separately.

11.4.3 Sole signatory on a bank account is not permitted except for cheques where one signatory may sign for amounts of up to £50,000.

11.5 Reconciliations

11.5.1 The Financial Accounting & Governance Manager is responsible for bank reconciliations.

11.5.2 The reconciliation process around certain bank accounts has been assigned to Treasury. For those accounts, Treasury will ensure that all bank accounts are reconciled to the underlying accounting records and all reconciling items are identified and cleared as appropriate, in a timely manner.

11.5.3 The HoTTI will ensure that all Treasury-owned reconciliations have been properly carried out and provided to the relevant staff members reporting to the POL FD in accordance with prescribed deadlines.

POL00423454

11.6 **Delegated Authorities**

- *Approve amendments to existing operational banking facilities* - **CFOO**
- *Approve new operational banking facilities* - **CFOO**
- *Approve opening of new bank account* - **HoTTI**
- *Approve closure of bank account* - **HoTTI**

POL00423454

12 Payments

12.1 Manual Payments

12.1.1 Signing mandates are managed by Treasury and must be in place with a bank for any account on which cheques or similar manual payment instructions (e.g. direct debit mandates) are issued.

12.1.2 Cheques or other manual payment instructions up to £50,000 may be signed by one signatory. Cheques or other manual payment instructions greater than £50,000 must be signed by two signatories.

12.1.3 It is the responsibility of the paying department to ensure that there is adequate segregation of duties with regard to the preparation of manual payment instructions and cheques and that written procedures governing the processing of payments are in place.

12.1.4 Cheque books should be kept in a secure place.

12.1.5 Paying-in books should also be kept in a secure place. To prevent credits being made to unauthorised accounts, only pre-printed paying-in slips should be used when paying in cheques.

12.1.6 **Delegated Authorities**

- *Sign manual payment instruction - < £50k* - **Any 1 member of Banking Authorisation Panel**
- *Sign manual payment instruction - > £50k* - **Any 2 members of Banking Authorisation Panel**

12.2 Computer-Generated Cheque Payments

12.2.1 There should be adequate physical security over the hardware and software used for the preparation of computer-generated cheques. Detailed records should be kept of cheque stationery utilised and any missing cheque numbers investigated. A monetary limit should be set for the maximum value of any computer-generated or machine-signed cheque.

12.3 Manually-Instructed Payments

12.3.1 Where any use is made of electronic payment systems via a bank, staff must ensure that adequate written control procedures exist to ensure that the bank will only respond to verified requests from authorised personnel, these include:

- the use of code words;
- answer-back arrangements with the bank calling back to an authorised signatory (other than an authorised signatory who has signed the request);
- requests by telephone for transfers to be supported by a written request, signed in accordance with the mandate, received by the bank prior to dispatch of funds;
- transfer requests should only be sent on company headed notepaper, or pre-printed forms unique to the Group.

12.3.2 Treasury must approve any proposal to start using an internet banking platform and undertake a detailed security review.

12.3.3 If a bank requests any Group employee to sign an indemnity giving protection to the bank in respect of payment instructions actioned by the bank, then this document must be forwarded to Treasury for review and approval prior to signature.

POL00423454

12.4 Electronic Transfers

12.4.1 Electronic Funds Transfer (BACS/CHAPS/Faster Payments) is the preferred means of payment. Where internet banking systems are used to make such payments, care must be taken to ensure that there is adequate physical security over the system to prevent unauthorised access. The networking of internet banking systems should be approved collectively by the Treasury and IT departments.

12.4.2 It is the responsibility of Treasury to ensure that there is adequate segregation of duties in relation to initiating, authorising and releasing payments.

12.4.3 The authorisation process must be fully documented. Non-compliance with the agreed authorisation procedures will be referred to the CFOO and ARC Committee and is considered a serious breach of control.

12.4.4 BACS limits will be negotiated with the bank by Treasury and will be communicated to the relevant business unit. Any request for an increase to a BACS limit must be made by Treasury.

12.4.5 Any recommendations by a bank providing an internet banking system with regard to the control environment surrounding that system must be adhered to in all respects.

12.4.6 Treasury must approve any proposal to start using internet banking systems or other host-to-host solutions to initiate payments and ensure that a security review has been undertaken if appropriate.

12.4.7 **Delegated Authorities**

- *Release payment from Internet Banking System - < £50k* - **Any 1 Payment Panel (Internet Banking System)**
- *Release payment from Internet Banking System - > £50k* - **Any 2 Payment Panel (Internet Banking System)**
- *Release payment from Treasury Management System / SAP* - **Various (see Appendix C)**

POL00423454

13 Guarantees and Indemnities / Group Support

13.1 POL Support for Subsidiaries

13.1.1 POL may be asked to provide a letter of comfort, a letter of awareness or a direct guarantee or indemnity to a third party to support the activity of its subsidiaries[3]. Although a guarantee creates a contingent liability on POL it does not increase the overall liabilities of the Group. It is considered reasonable to meet such requests on behalf of a subsidiary.

13.1.2 Requests of this type will be reviewed on a case-by-case basis and POL will also consider whether it is more appropriate to issue a letter of comfort or letter of awareness. Generally such a guarantee will not have a cost for POL. The authority to approve and sign a direct guarantee to a commercial third-party for the benefit of any subsidiary must be approved in accordance with the Group Delegated Authorities around indemnities.

13.1.3 For the avoidance of doubt 13.1 does not apply to guarantees provided by POL in favour of subsidiaries in connection with the raising of third-party finance by subsidiaries. All such guarantees must be considered by the Board.

13.1.4 **Delegated Authorities**

- *Approve and execute a direct guarantee or indemnity to a commercial third party for the benefit of a subsidiary* - **See Group Delegated Authorities for Indemnities**

13.1.5 As of March 2019 POMS and Payzone Bill Payments Limited are the only subsidiaries of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such entities are considered to be subsidiaries under 2006 Companies Act, then 13.1 will also be applicable for guarantees or indemnities for the benefit of those subsidiaries.

13.2 Bank Guarantees

13.2.1 POL may provide a counter-guarantee to a bank to support a guarantee made by that bank to a third party (a "bank guarantee") on behalf of POL. Such a bank guarantee may be used to support financing provided by a third party or to support a commercial arrangement. Such an arrangement may create a contingent financial exposure for the Group.

13.2.2 *To Support Financing* - Where the bank guarantee is used to support a financing arrangement approval will be by the POL Board.

13.2.3 *To Support Commercial Activity* - Where the bank guarantee is being provided to support commercial activity the authority to approve and sign the guarantee to the bank must be approved in accordance with the Group Delegated Authorities around indemnities.

13.2.4 **Delegated Authorities**

- *Approve bank guarantee to support financing arrangement* - **Board**
- *Approve bank guarantee to support commercial arrangement* - **See Group Delegated Authorities for Indemnities**
- *Execute counter-guarantee to bank in support of commercial arrangement* - **See Group Delegated Authorities for Indemnities**

13.3 Government Support for the Group

13.3.1 From time-to-time the Group may be asked to obtain a letter of comfort, a letter of awareness or a guarantee from Government to support its activities. Such arrangements do not create a contingent liability of the Group.

13.3.2 Requests will be considered on a case-by-case basis and will require POL Board approval.

[3] *As defined under 2006 Companies Act.*

POL00423454

14 Regulatory Obligations

14.2 European Market Infrastructure Regulation ("EMIR")

14.2.1 Effective from January 2018, as a result of the changes introduced by MiFID II, the Group's derivative activity is subject to the requirements of EMIR.

14.2.2 POL is classified as a Non-Financial Counterparty "-" (an "NFC –")

14.2.3 As an NFC – EMIR places certain obligations on POL, namely:

a) *Reporting Obligations* – POL must report its derivative contracts to a trade repository no later than the working day after execution.

b) *Risk Mitigation Techniques* – POL must: (i) confirm trades in a timely manner; (ii) have dispute resolution processes in place; and (iii) engage in portfolio reconciliation.

14.2.4 POL will delegate reporting to its counterparty in derivatives transactions and will only execute derivative transactions with counterparties with which it has the appropriate delegated trade reporting agreements in place.

14.2.5 All trades will be confirmed by the end of the second day after execution.

14.2.6 POL will have ISDA agreements in place with all derivative counterparties to ensure that dispute resolution and portfolio reconciliation processes are documented.

POL00423454

15 ISDA Master Agreements

15.2 POL enters into ISDA[4] Master Agreements with potential derivative counterparties. The ISDA is an industry-standard agreement which governs the relationship between derivative counterparties and each transaction entered into under the ISDA. The key provisions of the ISDA include terms relating to payment and delivery obligations, termination rights, the close-out netting of transactions on termination, and representation and warranties. When executing derivative transactions POL enters into confirmations pursuant to the ISDA, which contain the economic terms of each transaction.

15.3 POL will only enter into derivative transactions with counterparties with which it has an ISDA agreement in place. POL will ensure that ISDA agreements are broadly similar in all material respects across counterparties. It is policy to standardise ISDAs where possible.

15.4 Only Treasury can negotiate ISDAs on behalf of POL.

15.4 **Delegated Authorities**

- *Agree changes to an ISDA Schedule* - **HoTTI**
- *Approve and execute ISDA agreement on behalf of POL* - **CFOO**

[4] *ISDA – International Swaps and Derivatives Association*

POL00423454

Section III - Governance and Reporting

16 Treasury Governance and Reporting

16.1 Governance

16.1.1 PO Treasury risks are governed through the following structures:

16.1.2 **POL Board:** Authority to approve policies and approval limits relating to treasury risk management resides with the Board. Treasury risk management includes but is not limited to the following: short-term liquidity management, long-term funding, counterparty risk management, foreign exchange exposure management and interest rate risk management. The Board will delegate authorities to facilitate the operation of treasury risk management and the daily operation of the Treasury function.

16.1.3 **ARC Committee**: Financial risk management policies and approval limits are recommended to the Board for approval by the ARC Committee.

16.1.4 **Risk and Compliance Committee ("RCC")**: Financial risk management policies will be presented to the RCC for noting prior to submission to the ARC.

16.1.5 **Treasury Committee:** Is part of the Operations Board and meets on a monthly basis to review the Treasury Report, review financial risks, report on headroom and working capital, and report on and recommend changes to policy to the ARC Committee as required. The Treasury Committee is composed of the CFOO, the POL FD, the HoTTI and Finance Director Financial Services. Other members of the Operations Board may attend from time-to-time.

16.1.6 **FX Currency Hedging Committee**: Meets monthly or more frequently as required from time-to-time to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy. The committee is composed of: the Director of Product; the Finance Director Financial Services and Telecoms; and the Head of Travel.

16.1.7 The Board has delegated the following specific authorities to the CFOO and POL FD.

CFOO:	• Approval of investment instrument limits • Approval of counterparty selection criteria • Approval of counterparties • Approval of counterparty limits
POL FD:	• Approval of counterparties • Approval of counterparty limits (within approved investment instrument limits)

16.1.8 The daily operation of treasury activity is delegated to the panels as shown on Appendix D. In all cases members of these panels will be appointed by the Treasury Committee.

16.1.9 Authority levels for write-offs are shown in Appendix F.

16.2 Treasury Management Reporting

16.2.1 The Treasury Report will be produced on a monthly basis. The contents of the report will include analysis of: note and coin inventory and how it is funded; insurance limits in cash centres; network cash holdings and inward rems; a monthly forecast update, including variance analysis for the prior period; Facility Headroom and Security Headroom; balances held in bank accounts; the net NRF Cap position; fx gains and losses; exposures to interest rate risks; treasury controls; as well as a summary of any project work currently being undertaken by Treasury.

16.2.2 The Treasury Committee will meet on a monthly basis as part of the Operations Board. It will review the Treasury Report and consider any other treasury risk management issues as required and make recommendations to the ARC.

POL00423454

16.2.3 Policy breaches will be immediately reported to the CFOO and the Group Director of Legal, Risk & Governance and, when considered appropriate, at the discretion of the CFOO, to the RCC and ARC.

16.2.4 Treasury KPIs will be reviewed regularly.

16.2.5 Authorities to drawdown under established facilities are laid out in Appendix E.

16.2.6 An additional authority matrix is shown in Appendix F that relates to various items which arise during the normal course of business and for which individual write-off authorities are required. Examples of such items, which will normally be provided for, include:

- ATM cash trapping and retract fraud;
- Travelers' Cheque fraud;
- Camelot scratch cards failures in stock control due to master data errors.

Alisdair Cameron
March 2019

POL00423454

Appendix A: Summary of Counterparty Relationships, Services & Exposures

Financial Institution Counterparty	Exposure Area	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Max. Current Estimated Exposure (£m)	Approved Limit (£m)	Comments
a) Corporate Treasury Activity										
Barclays Bank PLC	Investment of Surplus Cash Balances	**A**	**A-1**	**Stable**	**A**	**F1**	**Positive**	40.0	80.0	Either through bank term deposits or interest bearing accounts
	Mk-to-mkt of Derivatives									
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								40.0	**130.0**	
National Westminster Bank Plc	Investment of Surplus Cash Balances	**A-**	**A-2**	**Positive**	**A+**	**F1**	**Negative**	5.0	60.0	Either through bank term deposits or interest bearing accounts
	Committed Facilities									
	- £400m intra-day/£350m overnight facility							400.0	400.0	Exposure on undrawn amount of commitment
NatWest Markets Plc	Mk-to-mkt of Derivatives	**BBB+**	**A-2**	**Positive**	**A**	**F1**	**Negative**			
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								405.0	**510.0**	
Lloyds Bank Plc	Investment of Surplus Cash Balances	**A+**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	40.0	60.0	Either through bank term deposits or interest bearing accounts
	Mk-to-mkt of Derivatives									
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								40.0	**110.0**	
Governor & Company of the Bank of Ireland	Mk-to-mkt of Derivatives	**BBB+**	**A-2**	**Positive**	**BBB**	**F2**	**Positive**			
	- FX							-	10.0	Trades booked through Bank of Ireland First Currency Services (BOIFCS)
								-	**10.0**	
b) Other Client-related Activity										
Barclays Bank PLC	Banking Framework (1)							30.0		Exposure related to clearing and settlement of banking framework tranasactions
Bank of Ireland	ATM Withdrawals							135.0		Exposure related to cash withdrawls from ATMs
JP Morgan Europe Limited	Poca-related Flows							125.0		
GPUK LLP	Debit and Credit Card Processing (3)							75.0		One day exposure to GlobalPay relating to clearing of debit and credit card transactions

Notes:

(1) POL is also exposed to the failure of individual client banks under the Banking Framework to meet their obligations under the Link system.

(2) A short-term (2 day) exposure is created when a customer makes a paymnet to POL via cheque. As well as on the customer the exposure is also against the bank on which the cheque is drawn. The aggregated exposure across all banks is approx. £25m per c

(3) A short-term (1 day) exposure is created when a customer makes a payment to POL via debit or credit. As well as on the customer and GlobalPay the exposure is also against the card issuer. The aggregated exposure is approx. £75m per day.

POL00423454

Appendix B: CHAPS Banks

Bank of America (N.A)

Bank of England

Bank of Scotland (HBOS)

Barclays Bank PLC

Citibank N.A

CLS Bank International

Clydesdale Bank PLC

The Co-operative Bank PLC

Danske Bank

Deutsche Bank A.G

HSBC Limited

J.P. Morgan Chase Bank

Lloyds TSB Bank PLC

National Westminster Bank PLC

The Royal Bank of Scotland PLC

Santander UK PLC

Standard Chartered

State Street Bank

UBS A.G.

POL00423454

Appendix C: Delegated Authorities for Authorisation Panels

	Authorisation Panel	Delegated Authorities	Current Composition
Investment of Surplus Cash	Treasury Authorisation Panel	Approve investment of surplus cash balances - within policy Approve drawdowns - under existing credit facilities (up to 1 day)	Matrix securely maintained centrally by Treasury
	Dealing Panel	Propose investment of surplus cash balances Propose drawdowns - under credit existing facilities	Matrix securely maintained centrally by Treasury
Manual Payments	Banking Authorisation Panel *	Sign manual payment instruction (1) - < £50k - any 1 Banking Authorisation Panel member - > £50k - any 2 Banking Authorisation Panel members	Matrix securely maintained centrally by Treasury
Electronic Transfers	Payment Panel - (Internet Banking Systems) *	Release payment from internet banking system (2) - < £50k - any 1 Payment Panel (Internet Banking System) member - > £50k - any 2 Payment Panel (Internet Banking System) members	Matrix securely maintained centrally by Treasury
	Payment Panel - (Treasury Management System) ** *[BEIS Facility, NRF and file gateway payments]*	Release payment from TMS (2) - any 1 Treasury check AND - any 1 Banking Authorisation Panel OR Payment Panel member	Matrix securely maintained centrally by Treasury
	Payment Panel - (SAP) ** *[release of BACS payments]*	Release payment from SAP (2) - any 1 Amalgamated payment proposal AND - any 1 payment authoriser	Matrix securely maintained centrally by Treasury

(1) Cheques and direct debit instructions to bank - Banking Authorisation Panel members in accordance with mandates held by banks
(2) Aligned to authorisation rights in Internet Banking Systems / Treasury Management System / SAP

* *In respect of both the Banking Authorisation Panel and the various Payment Panels the lists are extensive and complex owing to the number of bank accounts used within the Group. The full listings are therefore not replicated here but are maintained and held securely by Treasury.*

** *In respect of the Treasury Management Systems and SAP, the controls around changes to master data (bank details), in particular around segregation of duties, are deemed to be strong enough that a two stage authorisation is not needed.*

9.1

POL00423454

Appendix D: Delegated Authorities for Drawdowns Under Credit Facilities

1. Approval of Drawdowns under BEIS Facility

Drawdown Amount	< £950m	< £950m	< £950m
Period of Drawdown	Up to 1 day	Over 1 day and up to 12 mths	over 12 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	*POL FD*	*CFOO*

2. Approval of Drawdowns Under Other External Borrowings (including the BEIS Short-term Facility)

Drawdown Amount	< £50m	< £50m	< £50m	< £50m
Period of Drawdown	Overnight	Up to 1 wk	up to 6 mths	over 6 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	*HoTTI*	*POL FD*	*CFOO*

3. Leasing and Contract Hire

Amount	< £50m	< £50m
Maturity	Up to 8 years	Over 8 years
Delegated Authority	*POL FD + CFOO*	*CFOO*

POL00423454

Appendix E: Individual Write-off Authority Levels

Authorities to write off provided-for items relating to external fraud and data errors:

Amount	< £1k	£1k to £10k	£10k to £100k	> £100k
Delegated Authority	*FSC Team Leader*	*FSC Senior Manager of Relevant Work Area*	*Head of FSC*	*CFOO*

POL00423454

Appendix F: Summary of Delegated Authorities

Separate attachment.

POL00423454

POST OFFICE LIMITED AND SUBSIDIARIES (THE "GROUP")

TREASURY RISK MANAGEMENT FRAMEWORK, POLICIES AND AUTHORITIES - MARCH 2019

		Page
I - Introduction		
1	Background	2
2	Policy Overview	3
II - Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity		
Key Policies		
3	Short-Term Cash and Liquidity Management	5
4	Medium and Long-term Funding Management	8
5	Counterparty Credit Risk Management	10
6	Investment Risk Management	12
7	Foreign Exchange Exposure Management	16
8	Interest Rate Exposure Management	18
9	Bank Relationship Management	19
10	Commodity Price Exposure Management	20
Other Guidelines		
11	Operational Banking	21
12	Payments	23
13	Guarantees and Indemnities / Group Support	25
14	Regulatory Obligations	26
15	ISDA Agreements	27
III - Governance and Reporting		
16	Treasury Governance and Reporting	28
APPENDICES		
A	Summary of Counterparty Relationships, Services and Exposures	30
B	CHAPS Banks	31
C	Delegated Authorities for Authorisation Panels	32
D	Delegated Authorities for Drawdowns under Credit Facilities	33
E	Individual Write-off Authority Levels	34
F	Summary of Delegated Authorities	35

POL00423454

I - Introduction

1. Background

1.1. This document sets out the risk management framework, policies and authorities adopted by Post Office Limited ("POL") and its subsidiaries (together the "Group") in relation to its treasury activities and is an update of the paper approved by the ARC Committee in March 2018. It is recognised that Post Office Management Services Limited ("POMS") is subject to regulatory and fiduciary obligations which require derogation from some of the following policies. POMS will determine where there is a conflict between its obligations and these policies and amendments will be agreed and documented. A service agreement will set out the treasury activities which will be carried out on behalf of POMS.

1.2 This document should be read in conjunction with the wider Group Delegated Authorities. For the avoidance of doubt, in the case of inconsistencies the Group Delegated Authorities will prevail.

1.3 The treasury risk management framework has been designed to:

- protect financial asset values;
- minimise income statement volatility;
- ensure financial obligations are met as they fall due;
- secure long-term funding to meet overall business objectives and shareholder return requirements;
- ensure regulatory obligations are met.

1.4 The key treasury risks are:

- *Short-term cash and liquidity risk* – the Group does not have sufficient short-term liquidity to meet payment obligations;
- *Medium and long-term funding risk* – the Group does not have sufficient committed long-term funding in place to meet business objectives and going concern obligations;
- *Counterparty credit risk* – a financial institution counterparty cannot meet its obligations to the Group. Such obligations may arise from: investing the Group's surplus cash balances (see investment risk, below); entering into derivatives transactions; entering into committed facility arrangements; and certain other commercial arrangements with clients.
- *Investment risk* – arising from investing the Group's surplus cash balances;
- *Foreign exchange risk* - arising from holding currency note inventory in branches and cash centres to meet on-demand requirements from customers;
- *Interest rate risk* – arising from the impact of changes in interest rates on the cost of funding, the returns earned on the investment of surplus cash, and the returns earned on the POca cash balances;
- *Bank relationship risk* – the Group does not manage its bank relationships in an appropriate manner;
- *Commodity price risk* – arising from the impact of changes in commodity prices on operational costs;
- *Settlement risk* – the risk that operational and business payments are not executed in accordance with agreed policies and procedures, are not settled in a timely manner or are exposed to the possibility of fraud;
- *Regulatory risk* – arising from POL failing to meet its regulatory obligations around its treasury activities;
- Proper recording of treasury transactions, including the reconciliation of bank statement balances to ledger balances in a timely manner;
- Loss or theft of cash.

1.5 In this document authorities have been delegated to the Chief Financial and Operating Officer (the "CFOO"), the POL Finance Director (the "POL FD"), and the Head of Treasury, Tax and Insurance (the "HoTTI"), being the roles and titles existing as at February 2019. Where titles change over time authorities will rest with those persons performing substantially the same roles. In any case of doubt confirmation will be provided by the Company Secretary.

POL00423454

2. Policy Overview

2.1 The Board is averse to treasury risk. The risk management framework and policies have been designed to reduce risk and concentrate on five principal areas to achieve this:

- **Market Risk**: to minimise any potential loss due to a change in market factors (e.g. interest rates, exchange rates or commodity prices);
- **Credit Risk**: to minimise any potential loss due to a change in the credit-worthiness of a counterparty;
- **Business Risk**: to minimise any potential loss due to economic factors;
- **Operational Risk**: to minimise any potential loss due to system, people, legal and other external events;
- **Regulatory Risk**: to minimise the risk that POL fails to meet its regulatory obligations around treasury activities.

2.2 Day-to-day operation of treasury policy and the activities of the Treasury function are the responsibility of the HoTTI, who reports to the POL FD. Treasury activities are reported on a monthly basis to the Treasury Committee, which is part of the Operations Board, for review and oversight. The composition and responsibilities of the Treasury Committee are set out in section 16.1.

2.3 Any proposed amendments to, or derogations from, policy will be considered in the Treasury Committee and approved by the Audit, Risk and Compliance ("ARC") Committee or, if appropriate, by the Board.

2.4 Treasury is responsible for the following activities. These activities will only be undertaken by Treasury unless an alternative arrangement has been formally approved by the ARC Committee or the Board:

- management of bank account structures to provide automated concentration of cash and/or offset of balances;
- management of the Group's short-term cash flow forecasting process;
- arrangement and management of short-term committed funding;
- monitoring the debt capital structure to ensure that the Group has sufficient funding to support medium and long-term forecast requirements and to minimise refinancing risks;
- management of short, medium and long-term borrowing requirements;
- providing input to and critical review of the Group's medium and long-term cash flow forecasting process;
- fulfilment of obligations under the rules of the Bank of England's Note Circulation Scheme;
- setting counterparty limits for the financial institutions with which Group does business;
- short-term liquidity management and the investment of surplus cash balances;
- executing FX hedges in accordance with the instructions of the FX Committee, using approved instruments to hedge out to a maximum of 6 weeks;
- monitoring net interest rate exposure;
- managing bank relationships, in relation to corporate treasury activity;
- monitoring exposure to commodity price volatility;
- executing payments and administrating payments systems;
- acting as a centre of excellence in providing guidance and advice on all operational banking, payments and other treasury-related matters;
- regularly reviewing mandates;
- ensuring adherence to internal controls around internet banking systems and security;
- ensuring adherence to treasury-related regulatory obligations.

2.5 Cash forecasting must be completed in accordance with Treasury's instructions and deadlines and will support short-term, medium-term and long-term forecasting with the current Strategic Plan of the Board (currently the 5-year plan to 2020/21). Any material variances are to be escalated to the POL FD.

2.6 Compliance with the treasury policies set out in this document is mandatory, subject to the derogations provided to POMS noted in 1.1 above.

POL00423454

2.7 **Delegated Authorities**

- *Approve treasury risk management framework, policies and authorities* - **ARC**
- *Approve amendments to or derogations from Treasury Risk Management Framework, Policies and Authorities* - **ARC**

POL00423454

II Detailed Policies for the Management of Financial and Other Risks Relating to Treasury Activity

Key Policies

3. Short-Term Cash and Liquidity Management

Business Context

3.1 On a daily basis the Group has significant operating, investing and financing cash flows across its bank accounts, arising in relation to client-related activity across our counters, and as well as its own business-related activity. Client-related inflows and outflows are material and volatile with approx. £65 billion of flows each year. Flows can vary significantly depending on the day of the week and time of year and can also be materially impacted by other factors, out of the Group's control, such as the weather. Even with appropriate long-term committed funding in place there is therefore a short-term liquidity risk that the Group does not have resources available to meet its day-to-day payment obligations as they fall due.

Risk Management Objectives

3.2 The objective of the short-term cash and liquidity management policy is to ensure that the Group has appropriate liquidity in the right place at the right time to meet its payment obligations as they fall due.

Main Policy Statement

3.3 Through a combination of efficient bank account structures and accurate short-term cash flow forecasting, together with access to appropriate levels of committed short-term liquidity, Treasury will ensure that the Group can meet its obligations as they fall due.

Supporting Policy Guidelines

3.4 Bank Account Structures

3.4.1 Where possible, Treasury will manage cash balances within pooling arrangements which enable cash to be efficiently and effectively concentrated and debit and credit balances to be offset. Business units are not permitted to operate bank accounts that are outside these pooling arrangements unless authorised in writing by Treasury.

9.1

3.4.2 **Delegated Authorities**

- *Approve addition of bank account to existing pooling arrangement* - **HoTTI**
- *Approve removal of bank account from existing pooling arrangement* - **HoTTI**
- *Approve creation of new pooling arrangement* - **POL FD**

3.5 Short-term Cash Flow Forecasting

3.5.1 Short-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its day-to-day payment obligations.

3.5.2 Treasury will prepare a short-term, daily rolling forecast of the utilisation of the BEIS Facility and the NRF. The forecast, by day, covers a period of up to two accounting periods. Treasury will issue:

- daily reporting to the HoTTI analysing variances of same-day and two-day forecasts to actuals;
- a weekly Liquidity Report to the CFOO and POL FD updating the forecast for the following week and providing a variance analysis for last week;
- a monthly Forecast Update to the CFOO and POL FD updating the forecast for the following two periods and providing a variance analysis for the last period.

3.5.3 The forecasts and variances will be reviewed on a daily basis by the HoTTI. Monthly

POL00423454

Forecast Updates will be included in the Treasury Report and reviewed by the Treasury Committee. The ARC will be updated by exception.

3.6 Committed Short-term Funding

3.6.1 Treasury's first responsibility is to ensure that sufficient liquidity and facilities are available to the Group to fund its operations. Funding is therefore negotiated and managed centrally and the management of individual cash pools will be dealt with by Treasury.

3.6.2 Short-term liquidity is managed as follows: POL has access to a £950m working capital facility provided by the Department of Business, Energy and Industrial Strategy ("BEIS") (the "BEIS Facility"). The BEIS Facility is available until March 2021. A utilisation request must be provided to BEIS two days before drawdown. Forecasting variances may lead to a shortfall between the amount drawn down and the actual amount required. The strategy to mitigate the risk of a shortfall between forecast and actual funding requirements is to hold a liquid investment reserve of £5m (the "Investment Reserve"). Historically POL has tended to overdraw the BEIS Facility because it did not have access to an emergency source of short-term funding other than the NRF. Any changes to the targeted investment reserve will be reported to the Treasury Committee in the monthly Treasury Report. Treasury can also use a £5m uncommitted overdraft facility with Barclays, use the NRF (see 3.6.3 below), or use the £50m short-term credit facility provided by BEIS (the "BEIS Short-term Facility") (see 3.6.6 below).

3.6.3 In addition, POL is a member of the Bank of England's Note Circulation Scheme (the "NCS"). The scheme allows POL to declare and sell eligible notes to the Bank of England (the "Bank") overnight with a commitment to buy those notes back from the Bank first thing the next morning. This reduces the Group's overnight funding requirement. The NCS rules require the provision of collateral to the Bank. Collateral is currently provided on behalf of POL under a Facilities Agreement entered into by POL with National Westminster Bank Plc[1] under which the bank makes available: a £400m intra-day facility; a £350m overnight NRF facility (for the purposes of providing overnight collateral to the Bank); and, a £1m collateral facility, used in connection with our crime insurance.

3.6.4 The NCS rules also require that POL has a crime insurance in place that is compliant with BoE requirements.

3.6.5 The amount available to be used under the NRF over the course of the Bank's financial year (to October) is constrained by a cap (the "Cap") that POL generates, mainly as a function of outward rems processed from its NCS cash centres. Treasury will monitor utilisation of the NRF against the Cap to ensure that no more than the Cap generated is used over the course of the year and that financial penalties are therefore avoided. Cap generation and NRF utilisation will be reported to the Treasury Committee on a monthly basis via the Treasury Report.

3.6.6 POL has arranged a £50m short-term credit facility with BEIS. The facility is available on a same-day basis up to 11:45 am.

3.6.7 Any new borrowings require Board approval. See 4 Medium and Long-term Funding Requirement.

3.6.8 The delegated authorities for drawdowns are set out in Appendix D and in 3.6.9 below.

3.6.9 **Delegated Authorities**

- *Approve change to Investment Reserve (nil to £20m / for up to 2 weeks)* - **HoTTI**
- *Approve change to Investment Reserve (up to £50m / for more 2 weeks)* - **CFOO**
- *Propose drawdown - under existing credit facilities* - **Dealing Panel**
- *Approve drawdown - under BEIS Facility* - **Various (see Appendix D)**
- *Approve drawdown - under other external borrowings, including the BEIS Short-term Facility (up to £50m)* - **Various (see Appendix D)**

[1] *These facilities were provided by Royal Bank of Scotland plc and were novated to National Westminster Bank Plc in 2018 as part of the restructuring of the bank as a response to the Government's ring-fencing requirements.*

POL00423454

3.7 Short-term Cash & Liquidity Arrangements with Subsidiaries of POL

3.7.1 From time to time subsidiaries[2] of POL may have surplus cash balances which they wish to deposit with POL or they may have short-term funding needs which can be satisfied by POL.

3.7.2 POL is permitted to take loans from or make loans to subsidiaries.

3.7.3 All loans will be documented.

3.7.4 Margins on loans will be agreed between POL and the subsidiary and will be on an arm's length basis.

3.7.5 For short-term loans and deposits up to 3 months, for amounts up to £20m, authority to agree margins and execute documentation, on behalf of POL only, is delegated to the CFOO.

3.7.6 For the avoidance of doubt, any loans to or from a subsidiary will require the approval of the subsidiary's Board.

3.7.7 At March 2019 POL has two subsidiaries: POMS and Payzone Bill Payments Limited. In the event that new subsidiaries are introduced into the Group structure then, provided such subsidiaries are subsidiaries under the 2006 Companies Act definition, then 3.7 will also be applicable for loans to/from those subsidiaries.

3.7.8 In 2019 POL is considering a legal entity optimisation project under which certain wholly-owned subsidiaries of POL will become sister companies of POL under a new holding company structure. Provided that loans to/from any sister company are permitted under the BEIS Facility and the entity's Articles of Association then they will be permitted under 3.7 and will be executed within delegated authorities set out herein.

3.7.9 From time-to-time POL may enter into short-term funding arrangements with First Rate Exchange Services Limited ("FRES") under which FRES provides a loan to POL to fund additional holdings of foreign currency note inventory. Such loans are also permitted under 3.7 and must be executed within the delegated authorities set out herein.

3.7.10 **Delegated Authorities**

- *Approve margin on intra-group loans to/from subsidiaries on behalf of POL (up to £20m / up to 3 months)* - **CFOO and Head of Tax**
- *Execute documentation for intra-group loans to/from subsidiaries on behalf of POL (up to £20m and up to 3 months)* - **CFOO**
- *Execute documentation for intra-group loans to/from subsidiaries on behalf of POL (over £20m or over 3 months)* - **POL Board**

[2] *As defined under 2006 Companies Act.*

POL00423454

4. Medium and Long-term Funding Management

Business Context

4.1 The Group develops its strategic objectives and prepares long-term business plans to meet those objectives. Such objectives will include the continued participation in the Bank of England's Note Circulation Scheme (the NCS") in order to ensure an adequate supply of notes for the branch network. The Group must ensure that it has sufficient committed long-term funding in place to meet these plans. There is a risk that the funding in place is not sufficient to achieve business objectives or to adequately withstand unforeseen changes to plans.

4.2 In order to present its financial statements on a going concern basis the Group must demonstrate, on an annual basis at each balance sheet date, that it has sufficient committed funding in place.

4.3 The Group's existing funding arrangements, including the facilities made available to enable participation in the NCS, are set out in 3 Short-term Cash and Liquidity Management.

Risk Management Objective

4.4 The objective of the medium and long-term funding management policy is to ensure that the Group has sufficient committed long-term funding in place to meet business objectives and going concern obligations.

Main Policy Statement

4.5 Through a combination of accurate medium and long-term cash flow forecasts and the monitoring of headroom, together with access to appropriate levels of long-term committed funding, the Group will ensure it has sufficient funding in place to meet business objectives and going concern obligations.

Supporting Policy Guidelines

4.6 Medium and Long-term Cash Flow Forecasting

4.6.1 Medium and long-term cash flow forecasting is an essential tool for the Group and enables it to have confidence that its committed facilities are sufficient to provide the liquidity needed to meet its business objectives and loan repayments.

4.6.2 Treasury will provide input to Group's medium and long-term forecasts, in particular the one-year and five-year strategic forecasts and in accordance with the current Board Strategy.

4.7 Funding Strategy

4.7.1 The CFOO and the POL FD will recommend to the Board the appropriate debt capital structure for the Group. The Group will have a debt maturity profile and funding structure adequate to meet its:

- business objectives, including growth strategy;
- going concern obligations.

4.7.2 The debt capital structure and maturity profile will be monitored by the CFOO and POL FD, and reviewed by the Treasury Committee to ensure that the Group has appropriate funding available to support its long-term plans. Where possible, the Group seeks to minimise its refinancing risk by adopting a range of maturities for its debt facilities. Maturity of existing facilities will be monitored to ensure that negotiations commence in a timely manner to extend or replace them.

4.8 Headroom

4.8.1 *Facility Headroom* - Facility Headroom is defined as the headroom available under the BEIS Facility. The Group will aim to maintain Facility Headroom of at least £200m (the "Facility Headroom Buffer"). Any reduction in Facility Headroom Buffer will require Board

POL00423454

approval. It will be monitored and reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.2 *Security Headroom* - Security Headroom is defined in the BEIS Facility. Treasury will also monitor the asset security headroom of the BEIS Facility. It will be reported in the monthly Treasury Report and the monthly Performance Report to the Board.

4.8.3 Treasury will use a combination of the short-term forecasts outlined in 3.5 above and the medium and long-term forecasts to monitor headroom.

4.8.4 **Delegated Authorities**

- Approve amendment to Facility Headroom Buffer - **Board**

4.9 Borrowing Policy

4.9.1 Borrowing is only permitted in sterling unless approved by the ARC.

4.9.2 Borrowing should only be incurred in accordance with the restrictions under clause 10 of POL's Articles of Association and may require shareholder approval.

4.9.3 Additional borrowing is only permitted in accordance with the constraints imposed under the BEIS Facility which limits borrowings as follows:

- the existing £950m BEIS Facility itself, or any refinancing thereof;
- up to £50m of additional finance or capital leases;
- up to £50m additional other borrowings.

Together with the facilities in place to support POL's participation in the NCS, namely:

- the £400m intra-day facility;
- the £350m overnight NRF facility.

4.9.4 **Delegated Authorities**

- Approve new medium and long-term funding - **Board**

POL00423454

5. Counterparty Credit Risk Management

Business Context

5.1 Counterparty credit risk arises where a financial institution counterparty cannot meet its obligations to the Group. Due to the nature of POL's business activities such exposures arise both as part of POL's normal corporate treasury activities and its other client-related activities. Exposures arise primarily as follows:

Corporate Treasury Activity

5.1.1 *Investment of Surplus Cash Balances* - Total exposure of approximately £5m but may increase up to £50m when the investment reserve is increased during holiday periods. (See 6. Investment Risk Management.)

5.1.2 *Mark-to-Market of Derivatives* - Derivative contracts (including FX swaps, FX forwards and interest rate swaps) where the mark-to-market position has moved in favour of POL such that the counterparty owes money to POL under the contract. Exposure arises due to changes in market rates. Because FX maturities are managed within one month total exposure is currently minimal.

5.1.3 *Committed Facilities* - Commitments made by a bank or other funding provider under facilities that remain undrawn by POL. Such facilities currently comprise: the BEIS Facility and the BEIS Short-term Facility; and, the £400m intra-day facility / £350m overnight NRF facility provided by National Westminster Bank Plc. The exposure relating to the BEIS Facility and the BEIS Short-term Facility is considered to be nil but there is an exposure on National Westminster Bank Plc that fluctuates during the day depending on how much is utilised under the facilities. Total exposure may be up to **£400m**.

Other Client-Related Activity

5.1.4 *Banking Framework* - Over-the-counter banking transaction services with retail and business customers. Transactions are cleared through the LINK system with daily settlement to POL received from Barclays Bank PLC this creates a daily net direct exposure to Barclays Bank PLC of up to **£30m**. In addition, POL would also be exposed to the failure of an individual client bank to meet its obligations under the LINK system.

5.1.5 *Debit and Credit Card Processing* - When a customer makes a payment to POL over-the-counter using either a debit card or a credit card settlement is received by POL via GPUK LLP ("GlobalPay") on the next business day. This creates a one-day credit exposure against GlobalPay. Total exposure fluctuates but is approximately **£75m**.

5.1.6 *Cheque Clearing* - when a customer makes a payment to POL using a cheque it creates a short-term exposure (up to two days) exposure against the bank on which the cheque is drawn. The total exposure on cheques is approximately **£25m** but this is disaggregated between the banks on which the cheques are drawn.

5.1.7 *Other Client-Related Activity* - Exposures arising from other client-related activities.

- ATM Withdrawals – Exposure to Bank of Ireland linked to cash withdrawals from ATMs. The exposure varies significantly, depending on the time of the year and day of the week, between **£20m** and up to **£135m**.

- POca Related Flows – Exposure to JPMorgan Europe Limited in respect of POca-related flows across POL counters. Flows between 13:00 on the previous day and 13:00 are aggregated and paid same day. The exposure fluctuates significantly depending on the day of the week and time of the year and is impacted by holiday periods and winter fuel payments. It can vary between **£20m** and up to **£125m**.

5.2 This policy focuses on counterparty credit risk arising from POL's corporate treasury activities.

POL00423454

Risk Management Objectives

5.3 The objective of the counterparty credit risk management policy is to minimise the Group's risk of loss in its corporate treasury activities as a result of the failure of a financial institution counterparty.

Main Policy Statement

5.4 Treasury will minimise the risk of loss due to the failure of a financial institution counterparty to meet its obligations by only entering into corporate treasury transactions with highly-rated counterparties and through credit approvals, limits and monitoring procedures.

Supporting Policy Guidelines

5.5 Treasury will only enter into corporate treasury transactions with appropriately approved financial institution counterparties.

5.6 The Group's corporate treasury-related credit risk arises primarily from the investment of surplus cash balances. For the purpose of the investment of surplus cash balances limits are allocated according to rating band rather than specified counterparty. Approved counterparties and sub-limits applicable to deposits (as at March 2019) are set out in 6 Investment Risk Management. Deposit limits will fluctuate with changes to credit ratings.

5.7 When monitoring the credit quality of counterparties Treasury will use short-term and long-term credit ratings from S&P and Fitch. The weaker of the two ratings will be used for decision-making purposes.

5.8 Approved counterparties and credit limits for other transaction types are set out in Appendix A.

5.9 New counterparties and limits may be approved from time to time. Treasury will make a recommendation to the Treasury Committee based on credit ratings for consideration and recommendation to the ARC.

5.10 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report. See 6. Investment Risk Management. Exposures to corporate treasury counterparty activities will be aggregated (including investment counterparties) and reported to the Treasury Committee on a monthly basis together with changes to credit ratings as part of the Treasury Report.

5.11 **Delegated Authorities**

- *Approve new financial institution counterparty* - **ARC**
- *Approve financial institution counterparty limit* - **ARC**
- *Approve temporary increase to financial institution counterparty limit* - **CFOO**

5.12 Note on the Implications of Ring-fencing - *Effective 1 January 2019 the major UK banks were required to implement the Government's ring-fencing requirements. In 2018 the Group's bank accounts and the £400m facilities with Royal Bank of Scotland Plc were transferred to National Westminster Bank Plc as part of the bank's restructuring to meet these requirements. From 2019 these accounts and facilities will sit inside the ring-fence. (It should be noted that the interest rate swap executed in April 2018 with NatWest Markets Plc sits outside the ring-fence.) Provided that the S&P and Fitch long-term and short-term credit ratings of National Westminster Bank Plc (or any other entity inside or outside the ring-fence) were the same as, or better than, Royal Bank of Scotland Plc then all references to Royal Bank of Scotland Plc were deemed to apply to National Westminster Bank Plc (or those other entities). This approach was also applied for Barclays Bank PLC and Lloyds Bank plc.*

POL00423454

6. Investment Risk Management

Business Context

6.1 Treasury manages short-term liquidity to target a cash buffer of £5m. The buffer is reduced to nil at period ends and can be increased up to £50m around holiday periods when liquidity risks are highest. This creates surplus cash balances that can be invested by Treasury.

Risk Management Objectives

6.2 The three core objectives of the Group's investment risk management policy are: (i) *security* – to preserve the principal sum; (ii) *liquidity* – to ensure investments are accessible when needed; (iii) *yield* – to optimise return on investments.

Main Policy Statement

6.3 The Group's overall consideration when depositing surplus cash balances is the preservation of the principal sum. Surplus cash balances will be invested by Treasury to optimise return, subject to counterparty credit risk considerations. These investments will not be subject to fluctuation in capital values.

Supporting Policy Guidelines

6.4 Permitted Investment Instruments - Treasury are permitted to use the following investment instruments: bank term deposits and deposits on interest-bearing accounts; money market funds ("MMFs"); and, when appropriate, deposits with the Debt Management Office ("DMO").

6.5 Permitted Currencies – Treasury will only invest in £-denominated instruments.

6.6 Approved Bank Counterparties and Deposit Limits - It is the Group's policy to establish and monitor limits for each of the counterparties that it makes investments with.

6.6.1 Limits for term deposits and interest-bearing accounts ("deposit limits") are based on credit rating bands rather than specific counterparties. Counterparties are allocated to bands based on the lower of the S&P and Fitch long-term credit rating as follows:

Credit Rating (1)	Approved Limit (£m)
AAA	120
AA+ to AA-	90
A+ to A-	60
BBB+	30
BBB and below	0

(1) Based on lower of S&P and Fitch long-term credit rating

6.6.2 Counterparties must have a long-term S&P or Fitch credit rating of at least BBB+ and a short-term S&P or Fitch credit rating of A2/F2.

6.6.3 Counterparties must also be a member of CHAPS (see Appendix C for a list of CHAPS banks).

9.1

POL00423454

6.6.4 Approved counterparties and deposit limits based on credit ratings as at January 2018 are:

Financial Institution Counterparty	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Approved Deposit Limit (£m)
Barclays Bank PLC	**A**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	80.0
National Westminster Bank Plc (1)	**A-**	**A-2**	**Positive**	**A+**	**F1**	**Negative**	60.0
NatWest Markets Plc (2)	**BBB+**	**A-2**	**Positive**	**A**	**F1**	**Negative**	Not applic.
Lloyds Bank Plc	**A+**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	60.0

(1) Entity inside ring-fence; (2) Entity outside ring-fence.

6.6.5 The deposit limits against individual institutions are expected to change with changes in credit ratings.

6.6.5 *Exception* - Barclays Bank PLC, as our cash management bank, is allocated an additional limit of £20m to allow for cash held as operational balances on bank accounts from time to time. Barclays' long-term rating of A+ would imply a deposit limit of £60m. The limit is increased to £80m.

6.7 Other

6.7.1 Unauthorised arbitrage is prohibited i.e. funds should not be specifically drawn down for investment purposes.

6.7.2 Only Treasury is permitted to invest surplus cash balances.

6.7.3 A proposal for the investment of surplus cash balances will be made by the Dealing Panel and approved by either the Treasury Authorisation Panel (see Appendix C – Delegated Authorities for Approval Panels) or in accordance with 6.11 below.

9.1

6.7 Deposit Tenor Limits

6.7.1 Deposits will be no longer than one month.

6.8 Money Market Fund Investment Criteria - It is the Group's policy to establish and monitor limits for each of the MMFs that it invests in.

6.8.1 The MMF must be rated by at least one of S&P and Fitch. If rated it must be rated AAAm by S&P and AAAmmf by Fitch.

6.8.2 POL's holding as a proportion of the fund size must not be greater than 10%.

6.8.3 MMFs must have a constant net asset value (CNAV) (also referred to as stable NAV) or a Variable Net Asset value (VNAV) (also referred to as accumulating NAV).

6.8.4 MMFs must have daily liquidity.

6.8.5 Investment is limited to £50m in any one MMF.

6.8.6 Investment in Prime Liquidity Funds is limited to £350m.

6.8.7 Investment in Government Funds is limited to £150m.

6.8.9 Where a single provider has segregated Prime Liquidity Funds and Government Funds, investments can be made in both MMFs subject to the limits above.

POL00423454

6.9 Approved MMFs and limits as at January 2018 are:

Name of Fund	Credit Rating S&P	Credit Rating Fitch	Asset Class	Currency	Name of Return	Fund Size (£m)	Approved Limit (£m)	Approved Limit / Fund Size (%)
IGNIS - Sterling Liquidity Fund (Standard Life)	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	14,400	50.0	0.3%
Invesco STIC Global Sterling Liquidity Portfolio	**AAAm**	**AAAmmf**	Prime	GBP	CNAV		50.0	#DIV/0!
Aberdeen Liquidity Fund (Lux) - Sterling Fund	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	14,400	50.0	0.3%
Blackrock - Institutional Sterling Liquidity Fund	**AAAm**	**AAAmmf**	Prime	GBP	CNAV	36,800	50.0	0.1%
Goldman Sachs - Sterling Liquid Reserves Fund	**AAAm**	**na**	Prime	GBP	CNAV	11,800	50.0	0.4%
Unallocated	**AAAm**	**AAAmmf**	Prime	GBP			100.0	
Sub-total - Prime Liquidity Funds							**350.0**	
Blackrock - Institutional Sterling Government Liquidity Fund	**AAAm**	**AAAmmf**	Government	GBP	CNAV	2,400	50.0	2.1%
Unallocated	**AAAm**	**AAAmmf**	Government	GBP			100.0	
Sub-total - Government Funds							**150.0**	

6.10 DMO Investment Criteria – The Group may invest with the DMO on an unlimited basis.

6.11 Operational Approvals - For each individual investment made approval is required as per the table below:

Investment Amount	< £300m	< £100m	< £50m	< £300m	< £50m	< £50m
Term of Investment	< 1 month	< 3 months	< 6 months	< 1 year	< 1 year	< 1 year
Delegated Authority	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*1 member from Treasury Authorisation Panel*	*POL FD*	*CFOO and 1 other POL Board Member*	*POL Board*

The POL FD is also authorised to approve investments with a maturity of up to 5 years for the purpose of providing collateral for the Note Circulation Scheme.

9.1

6.12 Monitoring

6.12.1 Exposures to investment counterparties will be monitored separately and reported to the HoTTI on a daily basis and to the Treasury Committee on a monthly basis in the Treasury Report.

6.13 Limit Breaches

6.13.1 When Treasury are aware of a potential breach in advance (for example, when Treasury choose to hold in excess of the authorised limit because no other investments opportunities are available) approval must be obtained from either the CFOO or the POL FD for a temporary increase to the limit. The temporary increase will normally be for no longer than one night.

6.13.2 When Treasury are not aware of the breach in advance (for example, where we receive more cash into our Barclays accounts than we had forecasted) Treasury will notify the CFOO of the breach immediately on becoming aware of it but in any event no later than close of business on the day after the breach occurred.

POL00423454

6.13.3 All limit breaches will be reported to the Treasury Committee in the monthly Treasury Report.

6.14 **Delegated Authorities**

- *Approve new investment counterparty - within approved credit rating bands* - **POL FD**
- *Approve changes to credit rating bands for deposit limits* - **ARC**
- *Approve temporary increase to investment counterparty deposit limit* - **CFOO**
- *Approve new permitted investment instrument* - **CFOO**
- *Propose investment of surplus cash balances* - **Dealing Panel**
- *Approve investment of surplus cash balances* - **Various (see 6.11)**

POL00423454

7 Foreign Exchange Exposure Management

Business Context

7.1 Foreign exchange risk principally arises from holding foreign currency note inventory in branches and cash centres to meet "on demand" requirements from customers. All currencies are purchased from FRES. The exchange risk arises from the time of purchase from FRES to the sale of currency to the customer. The size of balances on hand is determined by demand. POL holds note inventory balances in approximately 70 currencies. On average, currency holdings are c. £60m but can peak at over £100m during holiday periods.

Risk Management Objectives

7.2 The objective of the foreign exchange exposure management policy is to minimise the impact on the Group's income statement of foreign currency exposures arising from its day-to-day operations.

Main Policy Statement

7.3 Through a combination of periodic monitoring of foreign exchange exposures and entering into hedges within approved hedging bands the Group will ensure its exposure to fluctuations in exchange rates is minimised.

Supporting Policy Guidelines

7.4 The Head of Travel Money analyses the report of foreign currency note holdings in the network which is prepared by Supply Chain and the daily reports of foreign currency holdings provided by Treasury.

7.5 A monthly meeting of the FX Committee is held, attended by: the Director of Product; the Finance Director Financial Services and Telecoms; and the Head of Travel. The meeting is held to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy outlined below.

7.6 Detailed foreign exchange risk management policy statements

7.6.1 EUR and USD holdings will be hedged 100%; currencies with exposures over £1.5m will be hedged 90% to 100%; other currencies with exposures over £1 million will be hedged 70%.

7.6.2 At least 80% and no more than 120% of qualifying exposures will be hedged based on the average of (1) the previous period's actual holdings and (2) the forecast for one month forward.

7.6.3 Hedges will be closed out and reset to periods between two weeks and five weeks. Longer-dated hedges will be set to mature at a monthend and will be revalued at each intervening month end based upon the mark-to-market valuation provided by the hedging bank.

7.6.4 Hedging will be conducted with counterparties approved by the Treasury Committee (see 5 Counterparty Credit Risk Management).

7.6.5 Trades will be executed at a pre-arranged margin with all counterparties.

7.6.6 The maturity of financial instruments used to hedge foreign exchange exposures will normally be about a month but can be no longer than six weeks.

7.6.7 Permitted Instruments - Foreign currency exposures can only be hedged using foreign currency outright forwards or swaps.

7.6.8 FX hedging instruments can only be used to hedge exposures generated by holding currencies to meet on-demand transactions by customers.

POL00423454

7.7 Latest currency holdings and hedges will be reviewed at the end of each period immediately before the maturity of the monthly hedges by Financial Director Financial Services and Telecoms and the Head of POL Travel.

7.8 On a monthly basis the Finance Director Financial Services and Telecoms will report to the Treasury Committee on the gain or loss on foreign currency holdings.

7.9 From time-to-time POL may enter into short-term funding arrangements with First Rate Exchange Services Limited ("FRES") under which FRES provides a loan to POL to fund additional holdings of foreign currency note inventory. For permissions and authorities in connection with such loans see 3.7.9.

7.10 Any proposed changes to the policies above will be presented to the ARC Committee for approval.

7.11 **Delegated Authorities**

- *Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee* - **Treasury**
- *Approve new permitted FX hedging instrument* - **CFOO**
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – up to £50m* - **CFOO**
- *Approve FX hedge trades for exposures not created by currency note inventory holdings – above £50m* - **Board**

POL00423454

8 Interest Rate Exposure Management

Business Context

8.1 The Group is exposed to changes in interest rates via its Libor-linked funding and the returns it earns on cash balances. Increases in interest rates will increase the Group's cost of funding and increase the return it earns on cash, mainly linked to Post Office card account ("POca") balances.

8.2 The Group's funding is via the BEIS Facility maturing in 2021 and the NRF. Interest rates on both facilities are linked to Libor. POL also earns commission (credited to revenue) on the balances of benefit payments held by JP Morgan, the POca cash balances. The commission interest received is also linked to Libor. The interest receivable on the POca cash balances has historically exceeded the interest payable on POL's borrowings and is expected to do so for the foreseeable future, despite the long-term decline of POca cash balances. The interest payable on POL's funding is a natural hedge of the commission interest receivable.

Risk Management Objectives

8.3 The objective of the interest rate risk management policy is to minimise exposures to income statement impacts of changes in interest rates.

Main Policy Statement

8.4 The Group will monitor its exposures to changes in interest rates on a regular basis and recommend hedging strategies, if appropriate.

Supporting Policy Guidelines

8.5 Treasury will obtain forecasts of interest payable / commission receivable and the net interest rate exposure will be monitored by Treasury and, if appropriate, a proposal to hedge the exposure will be put to the Treasury Committee prior to approval by the Board.

8.6 The suitability and effectiveness of the interest rate risk management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

8.7 Permitted Instruments - Hedging will be by way of interest rate swaps. Other instruments may be approved by the ARC on a case-by-case basis.

8.8 The Government's Managing Public Money Guidelines allow organisations to consider the use of derivatives but require them to consider their use carefully especially to assess value for money. The Guidelines require POL to consult its sponsoring department / HM Treasury before executing any derivative for the first time.

8.9 **Delegated Authorities**

- *Approve new permitted interest rate hedging instrument* - **ARC**
- *Approve execution of interest rate hedging strategy* - **Board**

POL00423454

9. Bank Relationship Management

Business Context

9.1 Good long-term relationships with banks are crucial to the success of the Group around its corporate treasury activities. The Group requires support from banks across all its treasury activities and this support is particularly important for the provision of: short-term liquidity, including operational overdrafts; credit facilities to enable continued participation in the Note Circulation Scheme; and, FX instruments and other derivatives, requiring credit to be extended.

9.2 Due to the UK-focused nature of the Group, the limited requirement for external funding and a small amount of ancillary treasury business, the Group has historically focussed on building relationships with a small group of UK clearing banks.

Risk Management Objective

9.3 The objective of the bank relationship management policy is to establish, maintain and develop efficient and effective banking relationships with a core group of banks to provide the Group with long-term banking support irrespective of short-term business conditions and financial market turbulence.

Main Policy Statement

9.4 The Group will seek to build long-term relationships with two to three of the UK clearing banks.

Supporting Policy Guidelines

9.5 It is the Group's policy to build long-term relationships with providers of banking services and facilities in order to maximise mutual advantage. In allocating new business opportunities, preference will generally be given to banks where a relationship already exists, but this does not preclude the use of other banks identified by Treasury should it be appropriate. Any new relationships will be reported to the Treasury Committee in the monthly Treasury Report for approval.

9.6 Current counterparty relationships, including banks, are listed in Appendix B.

9.7 Management of the Group's bank relationships is the responsibility of the HoTTI and the Chief Financial and Operations Officer ("CFOO"). Bank selection will be determined by a number of factors, including service, price, product range, geographic spread and willingness to provide services. The decision to develop a new relationship will rest with the Treasury Committee.

9.8 From time to time POL may require that banking partners enter into Non-Disclosure Agreements ("NDAs") to protect Group-sensitive information. Approval will be required by the CFOO.

9.9 **Delegated Authorities**

- *Approve entering into relationship with new bank* - **Treasury Committee**
- *Approve entering into relationship with new bank (prior to Treasury Committee approval)* - **CFOO**
- *Approve entering into NDA with bank* - **CFOO**

POL00423454

10 Commodity Price Exposure Management

Business Context

10.1 The Group is exposed to movements in the price of diesel, gas and electricity used throughout the business.

Risk Management Objectives

10.2 The objective of the commodity price exposure management policy is to minimise income statement volatility due to changes in commodity prices.

Main Policy Statement

10.3 Treasury will monitor exposures to these commodities and forecast price movements and may recommend hedging action to the Treasury Committee or directly to the CFOO to protect the Group from adverse price movements.

Supporting Policy Guidelines

10.4 The CFOO is authorised to hedge each commodity, where it is believed to be economic to do so, up to a maximum of 3 years based on forecast future usage.

10.5 Permitted Instruments - permitted hedging instruments are spot purchases, currency deposits, forward contracts, call options, matched options (e.g. cylinders) and swaps. Futures will not be used without specific authority of the CFOO.

10.6 The Group will designate commodity cash flow hedges against forecast underlying exposures. Unrealised gains and losses on hedges will be deferred in reserves. This will be recycled to the income statement when the hedge matures to match forecast expenditure.

10.7 The suitability and effectiveness of the commodity price exposure management policy will be reviewed at each Treasury Committee meeting. Any proposed changes will be reported to the ARC Committee for approval and submission to the Board.

10.8 **Delegated Authorities**

- *Execute commodity price hedges within policy* - **Treasury**
- *Approve new commodity price hedge counterparty* - **CFOO**
- *Approve execution of commodity price hedge within policy* - **HoTTI**

POL00423454

Other Guidelines

11. Operational Banking

11.1 Bank Facilities

11.1.1 Treasury is responsible for the negotiation of all operational banking facilities and any changes to existing operational facilities. Such facilities include overdrafts, fx lines, BACS limits, intra-day limits and any similar arrangements. Directorates do not have the authority to negotiate or commit to any new operational banking facilities without prior approval from Treasury and are not authorised to undertake any discussions regarding credit lines.

11.1.2 All changes to existing operational banking facilities or any new operational banking facilities must be agreed by the CFOO.

11.2 Interest and Bank Charges

11.2.1 Bank transaction charges will be negotiated by Treasury to ensure minimum cost to the Group. Charges incurred will be reviewed by Treasury to ensure that the activity levels and unit costs applied by the banks to calculate charges are in accordance with agreed tariffs. Errors are to be notified directly to the bank.

11.3 Bank Accounts

11.3.1 It is the Group's policy to minimise the number of bank accounts it operates. Treasury will conduct a bi-annual audit to ensure it has an accurate record of bank accounts. Accounts not being utilised should be closed. This will be reconciled back to internal and bank records.

11.3.2 All new bank accounts will be approved by the HoTTI.

11.3.3 Where possible all accounts should be within a cash pooling arrangement. It is recognised that certain constraints apply to POMS cash, where restrictions may preclude pooling.

11.4 Bank Mandates

11.4.1 It is the Group's policy to standardise bank mandates wherever possible. Treasury will manage and administer all bank mandates centrally. Each bank account must be supported by a written, up-to-date mandate which is checked against a list of those colleagues leaving the business on a monthly basis.

11.4.2 Authority levels relating to internet banking systems will be documented separately.

11.4.3 Sole signatory on a bank account is not permitted except for cheques where one signatory may sign for amounts of up to £50,000.

11.5 Reconciliations

11.5.1 The Financial Accounting & Governance Manager is responsible for bank reconciliations.

11.5.2 The reconciliation process around certain bank accounts has been assigned to Treasury. For those accounts, Treasury will ensure that all bank accounts are reconciled to the underlying accounting records and all reconciling items are identified and cleared as appropriate, in a timely manner.

11.5.3 The HoTTI will ensure that all Treasury-owned reconciliations have been properly carried out and provided to the relevant staff members reporting to the POL FD in accordance with prescribed deadlines.

POL00423454

11.6 **Delegated Authorities**

- *Approve amendments to existing operational banking facilities* - **CFOO**
- *Approve new operational banking facilities* - **CFOO**
- *Approve opening of new bank account* - **HoTTI**
- *Approve closure of bank account* - **HoTTI**

POL00423454

12 Payments

12.1 Manual Payments

12.1.1 Signing mandates are managed by Treasury and must be in place with a bank for any account on which cheques or similar manual payment instructions (e.g. direct debit mandates) are issued.

12.1.2 Cheques or other manual payment instructions up to £50,000 may be signed by one signatory. Cheques or other manual payment instructions greater than £50,000 must be signed by two signatories.

12.1.3 It is the responsibility of the paying department to ensure that there is adequate segregation of duties with regard to the preparation of manual payment instructions and cheques and that written procedures governing the processing of payments are in place.

12.1.4 Cheque books should be kept in a secure place.

12.1.5 Paying-in books should also be kept in a secure place. To prevent credits being made to unauthorised accounts, only pre-printed paying-in slips should be used when paying in cheques.

12.1.6 **Delegated Authorities**

- *Sign manual payment instruction - < £50k* - **Any 1 member of Banking Authorisation Panel**
- *Sign manual payment instruction - > £50k* - **Any 2 members of Banking Authorisation Panel**

12.2 Computer-Generated Cheque Payments

12.2.1 There should be adequate physical security over the hardware and software used for the preparation of computer-generated cheques. Detailed records should be kept of cheque stationery utilised and any missing cheque numbers investigated. A monetary limit should be set for the maximum value of any computer-generated or machine-signed cheque.

12.3 Manually-Instructed Payments

12.3.1 Where any use is made of electronic payment systems via a bank, staff must ensure that adequate written control procedures exist to ensure that the bank will only respond to verified requests from authorised personnel, these include:

- the use of code words;
- answer-back arrangements with the bank calling back to an authorised signatory (other than an authorised signatory who has signed the request);
- requests by telephone for transfers to be supported by a written request, signed in accordance with the mandate, received by the bank prior to dispatch of funds;
- transfer requests should only be sent on company headed notepaper, or pre-printed forms unique to the Group.

12.3.2 Treasury must approve any proposal to start using an internet banking platform and undertake a detailed security review.

12.3.3 If a bank requests any Group employee to sign an indemnity giving protection to the bank in respect of payment instructions actioned by the bank, then this document must be forwarded to Treasury for review and approval prior to signature.

POL00423454

12.4 Electronic Transfers

12.4.1 Electronic Funds Transfer (BACS/CHAPS/Faster Payments) is the preferred means of payment. Where internet banking systems are used to make such payments, care must be taken to ensure that there is adequate physical security over the system to prevent unauthorised access. The networking of internet banking systems should be approved collectively by the Treasury and IT departments.

12.4.2 It is the responsibility of Treasury to ensure that there is adequate segregation of duties in relation to initiating, authorising and releasing payments.

12.4.3 The authorisation process must be fully documented. Non-compliance with the agreed authorisation procedures will be referred to the CFOO and ARC Committee and is considered a serious breach of control.

12.4.4 BACS limits will be negotiated with the bank by Treasury and will be communicated to the relevant business unit. Any request for an increase to a BACS limit must be made by Treasury.

12.4.5 Any recommendations by a bank providing an internet banking system with regard to the control environment surrounding that system must be adhered to in all respects.

12.4.6 Treasury must approve any proposal to start using internet banking systems or other host-to-host solutions to initiate payments and ensure that a security review has been undertaken if appropriate.

12.4.7 **Delegated Authorities**

- *Release payment from Internet Banking System - < £50k* - **Any 1 Payment Panel (Internet Banking System)**
- *Release payment from Internet Banking System - > £50k* - **Any 2 Payment Panel (Internet Banking System)**
- *Release payment from Treasury Management System / SAP* - **Various (see Appendix C)**

POL00423454

13 Guarantees and Indemnities / Group Support

13.1 POL Support for Subsidiaries

13.1.1 POL may be asked to provide a letter of comfort, a letter of awareness or a direct guarantee or indemnity to a third party to support the activity of its subsidiaries[3]. Although a guarantee creates a contingent liability on POL it does not increase the overall liabilities of the Group. It is considered reasonable to meet such requests on behalf of a subsidiary.

13.1.2 Requests of this type will be reviewed on a case-by-case basis and POL will also consider whether it is more appropriate to issue a letter of comfort or letter of awareness. Generally such a guarantee will not have a cost for POL. The authority to approve and sign a direct guarantee to a commercial third-party for the benefit of any subsidiary must be approved in accordance with the Group Delegated Authorities around indemnities.

13.1.3 For the avoidance of doubt 13.1 does not apply to guarantees provided by POL in favour of subsidiaries in connection with the raising of third-party finance by subsidiaries. All such guarantees must be considered by the Board.

13.1.4 **Delegated Authorities**

- *Approve and execute a direct guarantee or indemnity to a commercial third party for the benefit of a subsidiary* - **See Group Delegated Authorities for Indemnities**

13.1.5 As of March 2019 POMS and Payzone Bill Payments Limited are the only subsidiaries of POL. In the event that new subsidiaries are introduced into the Group structure then, provided such entities are considered to be subsidiaries under 2006 Companies Act, then 13.1 will also be applicable for guarantees or indemnities for the benefit of those subsidiaries.

13.2 Bank Guarantees

13.2.1 POL may provide a counter-guarantee to a bank to support a guarantee made by that bank to a third party (a "bank guarantee") on behalf of POL. Such a bank guarantee may be used to support financing provided by a third party or to support a commercial arrangement. Such an arrangement may create a contingent financial exposure for the Group.

13.2.2 *To Support Financing* - Where the bank guarantee is used to support a financing arrangement approval will be by the POL Board.

13.2.3 *To Support Commercial Activity* - Where the bank guarantee is being provided to support commercial activity the authority to approve and sign the guarantee to the bank must be approved in accordance with the Group Delegated Authorities around indemnities.

13.2.4 **Delegated Authorities**

- *Approve bank guarantee to support financing arrangement* - **Board**
- *Approve bank guarantee to support commercial arrangement* - **See Group Delegated Authorities for Indemnities**
- *Execute counter-guarantee to bank in support of commercial arrangement* - **See Group Delegated Authorities for Indemnities**

13.3 Government Support for the Group

13.3.1 From time-to-time the Group may be asked to obtain a letter of comfort, a letter of awareness or a guarantee from Government to support its activities. Such arrangements do not create a contingent liability of the Group.

13.3.2 Requests will be considered on a case-by-case basis and will require POL Board approval.

[3] *As defined under 2006 Companies Act.*

POL00423454

14 Regulatory Obligations

14.2 European Market Infrastructure Regulation ("EMIR")

14.2.1 Effective from January 2018, as a result of the changes introduced by MiFID II, the Group's derivative activity is subject to the requirements of EMIR.

14.2.2 POL is classified as a Non-Financial Counterparty "-" (an "NFC –")

14.2.3 As an NFC – EMIR places certain obligations on POL, namely:

a) *Reporting Obligations* – POL must report its derivative contracts to a trade repository no later than the working day after execution.

b) *Risk Mitigation Techniques* – POL must: (i) confirm trades in a timely manner; (ii) have dispute resolution processes in place; and (iii) engage in portfolio reconciliation.

14.2.4 POL will delegate reporting to its counterparty in derivatives transactions and will only execute derivative transactions with counterparties with which it has the appropriate delegated trade reporting agreements in place.

14.2.5 All trades will be confirmed by the end of the second day after execution.

14.2.6 POL will have ISDA agreements in place with all derivative counterparties to ensure that dispute resolution and portfolio reconciliation processes are documented.

POL00423454

15 ISDA Master Agreements

15.2 POL enters into ISDA[4] Master Agreements with potential derivative counterparties. The ISDA is an industry-standard agreement which governs the relationship between derivative counterparties and each transaction entered into under the ISDA. The key provisions of the ISDA include terms relating to payment and delivery obligations, termination rights, the close-out netting of transactions on termination, and representation and warranties. When executing derivative transactions POL enters into confirmations pursuant to the ISDA, which contain the economic terms of each transaction.

15.3 POL will only enter into derivative transactions with counterparties with which it has an ISDA agreement in place. POL will ensure that ISDA agreements are broadly similar in all material respects across counterparties. It is policy to standardise ISDAs where possible.

15.4 Only Treasury can negotiate ISDAs on behalf of POL.

15.4 **Delegated Authorities**

- *Agree changes to an ISDA Schedule* - **HoTTI**
- *Approve and execute ISDA agreement on behalf of POL* - **CFOO**

[4] *ISDA – International Swaps and Derivatives Association*

POL00423454

Section III - Governance and Reporting

16 Treasury Governance and Reporting

16.1 Governance

16.1.1 PO Treasury risks are governed through the following structures:

16.1.2 **POL Board:** Authority to approve policies and approval limits relating to treasury risk management resides with the Board. Treasury risk management includes but is not limited to the following: short-term liquidity management, long-term funding, counterparty risk management, foreign exchange exposure management and interest rate risk management. The Board will delegate authorities to facilitate the operation of treasury risk management and the daily operation of the Treasury function.

16.1.3 **ARC Committee**: Financial risk management policies and approval limits are recommended to the Board for approval by the ARC Committee.

16.1.4 **Risk and Compliance Committee ("RCC")**: Financial risk management policies will be presented to the RCC for noting prior to submission to the ARC.

16.1.5 **Treasury Committee:** Is part of the Operations Board and meets on a monthly basis to review the Treasury Report, review financial risks, report on headroom and working capital, and report on and recommend changes to policy to the ARC Committee as required. The Treasury Committee is composed of the CFOO, the POL FD, the HoTTI and Finance Director Financial Services. Other members of the Operations Board may attend from time-to-time.

16.1.6 **FX Currency Hedging Committee**: Meets monthly or more frequently as required from time-to-time to confirm the value of hedges and timescales of hedges in accordance with the FX risk management policy. The committee is composed of: the Director of Product; the Finance Director Financial Services and Telecoms; and the Head of Travel.

16.1.7 The Board has delegated the following specific authorities to the CFOO and POL FD.

CFOO:	• Approval of investment instrument limits • Approval of counterparty selection criteria • Approval of counterparties • Approval of counterparty limits
POL FD:	• Approval of counterparties • Approval of counterparty limits (within approved investment instrument limits)

16.1.8 The daily operation of treasury activity is delegated to the panels as shown on Appendix D. In all cases members of these panels will be appointed by the Treasury Committee.

16.1.9 Authority levels for write-offs are shown in Appendix F.

16.2 Treasury Management Reporting

16.2.1 The Treasury Report will be produced on a monthly basis. The contents of the report will include analysis of: note and coin inventory and how it is funded; insurance limits in cash centres; network cash holdings and inward rems; a monthly forecast update, including variance analysis for the prior period; Facility Headroom and Security Headroom; balances held in bank accounts; the net NRF Cap position; fx gains and losses; exposures to interest rate risks; treasury controls; as well as a summary of any project work currently being undertaken by Treasury.

16.2.2 The Treasury Committee will meet on a monthly basis as part of the Operations Board. It will review the Treasury Report and consider any other treasury risk management issues as required and make recommendations to the ARC.

POL00423454

16.2.3 Policy breaches will be immediately reported to the CFOO and the Group Director of Legal, Risk & Governance and, when considered appropriate, at the discretion of the CFOO, to the RCC and ARC.

16.2.4 Treasury KPIs will be reviewed regularly.

16.2.5 Authorities to drawdown under established facilities are laid out in Appendix E.

16.2.6 An additional authority matrix is shown in Appendix F that relates to various items which arise during the normal course of business and for which individual write-off authorities are required. Examples of such items, which will normally be provided for, include:

- ATM cash trapping and retract fraud;
- Travelers' Cheque fraud;
- Camelot scratch cards failures in stock control due to master data errors.

Alisdair Cameron
March 2019

POL00423454

Appendix A: Summary of Counterparty Relationships, Services & Exposures

Financial Institution Counterparty	Exposure Area	Credit Rating S&P Long-term	S&P Short-term	S&P Outlook	Fitch Long-term	Fitch Short-term	Fitch Outlook	Max. Current Estimated Exposure (£m)	Approved Limit (£m)	Comments
a) Corporate Treasury Activity										
Barclays Bank PLC	Investment of Surplus Cash Balances	**A**	**A-1**	**Stable**	**A**	**F1**	**Positive**	40.0	80.0	Either through bank term deposits or interest bearing accounts
	Mk-to-mkt of Derivatives									
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								40.0	**130.0**	
National Westminster Bank Plc	Investment of Surplus Cash Balances	**A-**	**A-2**	**Positive**	**A+**	**F1**	**Negative**	5.0	60.0	Either through bank term deposits or interest bearing accounts
	Committed Facilities									
	- £400m intra-day/£350m overnight facility							400.0	400.0	Exposure on undrawn amount of commitment
NatWest Markets Plc	Mk-to-mkt of Derivatives	**BBB+**	**A-2**	**Positive**	**A**	**F1**	**Negative**			
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								405.0	**510.0**	
Lloyds Bank Plc	Investment of Surplus Cash Balances	**A+**	**A-1**	**Stable**	**A+**	**F1**	**Negative**	40.0	60.0	Either through bank term deposits or interest bearing accounts
	Mk-to-mkt of Derivatives									
	- FX							-	10.0	
	- Interest Rate Swaps							-	15.0	
								40.0	**110.0**	
Governor & Company of the Bank of Ireland	Mk-to-mkt of Derivatives	**BBB+**	**A-2**	**Positive**	**BBB**	**F2**	**Positive**			
	- FX							-	10.0	Trades booked through Bank of Ireland First Currency Services (BOIFCS)
								-	**10.0**	
b) Other Client-related Activity										
Barclays Bank PLC	Banking Framework (1)							30.0		Exposure related to clearing and settlement of banking framework tranasactions
Bank of Ireland	ATM Withdrawals							135.0		Exposure related to cash withdrawls from ATMs
JP Morgan Europe Limited	Poca-related Flows							125.0		
GPUK LLP	Debit and Credit Card Processing (3)							75.0		One day exposure to GlobalPay relating to clearing of debit and credit card transactions

Notes:

(1) POL is also exposed to the failure of individual client banks under the Banking Framework to meet their obligations under the Link system.

(2) A short-term (2 day) exposure is created when a customer makes a paymnet to POL via cheque. As well as on the customer the exposure is also against the bank on which the cheque is drawn. The aggregated exposure across all banks is approx. £25m per c

(3) A short-term (1 day) exposure is created when a customer makes a payment to POL via debit or credit. As well as on the customer and GlobalPay the exposure is also against the card issuer. The aggregated exposure is approx. £75m per day.

POL00423454

Appendix B: CHAPS Banks

Bank of America (N.A)

Bank of England

Bank of Scotland (HBOS)

Barclays Bank PLC

Citibank N.A

CLS Bank International

Clydesdale Bank PLC

The Co-operative Bank PLC

Danske Bank

Deutsche Bank A.G

HSBC Limited

J.P. Morgan Chase Bank

Lloyds TSB Bank PLC

National Westminster Bank PLC

The Royal Bank of Scotland PLC

Santander UK PLC

Standard Chartered

State Street Bank

UBS A.G.

POL00423454

Appendix C: Delegated Authorities for Authorisation Panels

	Authorisation Panel	Delegated Authorities	Current Composition
Investment of Surplus Cash	Treasury Authorisation Panel	Approve investment of surplus cash balances - within policy Approve drawdowns - under existing credit facilities (up to 1 day)	Matrix securely maintained centrally by Treasury
	Dealing Panel	Propose investment of surplus cash balances Propose drawdowns - under credit existing facilities	Matrix securely maintained centrally by Treasury
Manual Payments	Banking Authorisation Panel *	Sign manual payment instruction (1) - < £50k - any 1 Banking Authorisation Panel member - > £50k - any 2 Banking Authorisation Panel members	Matrix securely maintained centrally by Treasury
Electronic Transfers	Payment Panel - (Internet Banking Systems) *	Release payment from internet banking system (2) - < £50k - any 1 Payment Panel (Internet Banking System) member - > £50k - any 2 Payment Panel (Internet Banking System) members	Matrix securely maintained centrally by Treasury
	Payment Panel - (Treasury Management System) ** *[BEIS Facility, NRF and file gateway payments]*	Release payment from TMS (2) - any 1 Treasury check AND - any 1 Banking Authorisation Panel OR Payment Panel member	Matrix securely maintained centrally by Treasury
	Payment Panel - (SAP) ** *[release of BACS payments]*	Release payment from SAP (2) - any 1 Amalgamated payment proposal AND - any 1 payment authoriser	Matrix securely maintained centrally by Treasury

(1) Cheques and direct debit instructions to bank - Banking Authorisation Panel members in accordance with mandates held by banks
(2) Aligned to authorisation rights in Internet Banking Systems / Treasury Management System / SAP

* *In respect of both the Banking Authorisation Panel and the various Payment Panels the lists are extensive and complex owing to the number of bank accounts used within the Group. The full listings are therefore not replicated here but are maintained and held securely by Treasury.*

** *In respect of the Treasury Management Systems and SAP, the controls around changes to master data (bank details), in particular around segregation of duties, are deemed to be strong enough that a two stage authorisation is not needed.*

9.1

POL00423454

Appendix D: Delegated Authorities for Drawdowns Under Credit Facilities

1. Approval of Drawdowns under BEIS Facility

Drawdown Amount	< £950m	< £950m	< £950m
Period of Drawdown	Up to 1 day	Over 1 day and up to 12 mths	over 12 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	*POL FD*	*CFOO*

2. Approval of Drawdowns Under Other External Borrowings (including the BEIS Short-term Facility)

Drawdown Amount	< £50m	< £50m	< £50m	< £50m
Period of Drawdown	Overnight	Up to 1 wk	up to 6 mths	over 6 mths
Delegated Authority	*1 member from Treasury Authorisation Panel*	*HoTTI*	*POL FD*	*CFOO*

3. Leasing and Contract Hire

Amount	< £50m	< £50m
Maturity	Up to 8 years	Over 8 years
Delegated Authority	*POL FD + CFOO*	*CFOO*

POL00423454

Appendix E: Individual Write-off Authority Levels

Authorities to write off provided-for items relating to external fraud and data errors:

Amount	< £1k	£1k to £10k	£10k to £100k	> £100k
Delegated Authority	*FSC Team Leader*	*FSC Senior Manager of Relevant Work Area*	*Head of FSC*	*CFOO*

POL00423454

Appendix F: Summary of Delegated Authorities

Separate attachment.

POL00423454

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2019

	Reserved Matter	Ref.	Notes	Authorisation Panels														
				Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insuranc	Treasury Manager	Treasury Authorisation Panel	Dealing Panel	Payment Panels: Banking Auth. Panel	Payment Panels: Internet Banking Systems	Payment Panels: Treasury Mgt. System	Payment Panels: SAP
GENERAL	**General**																	
	Approve treasury risk management framework, policies and authorities	2.7	Must be			√												
	Approve amendments to or derogations from treasury risk management framework, policies and authorities (1)	2.7	Must be			√												
3. SHORT-TERM CASH AND LIQUIDITY MANAGEMENT	**Bank Account Structures**																	
	Approve addition of bank account to existing pooling arrangement	3.4.2	Any 1 from						√	√	√							
	Approve removal of bank account from existing pooling arrangement	3.4.2	Any 1 from						√	√	√							
	Approve creation of new pooling arrangement	3.4.2	Any 1 from						√	√								
	Committed Short-term Funding																	
	Approve change to Investment Reserve																	
	- in the range nil to £20m / for up to 2 weeks	3.6.8	Any 1 from						√	√	√							
	- up to £50m / for more than 2 weeks	3.6.8	Must be						√									
	Propose drawdown - under existing credit facilities	3.6.8	Any 1 from											√				
	Approve drawdown - under BEIS Facility																	
	- up to 1 day	3.6.8	Any 1 from						√	√	√		√					
	- over 1 day and up to 12 months	3.6.8	Any 1 from						√	√								
	- over 12 months	3.6.8	Must be						√									
	Approve drawdown - under Other External Borrowings (up to £50m)																	
	- overnight	3.6.8	Any 1 from						√	√	√		√					
	- up to 1 week	3.6.8	Any 1 from						√	√	√							
	- up to 6 months	3.6.8	Any 1 from						√	√								
	- over 6 months	3.6.8	Must be						√									
	Short-term Cash & Liquidity Arrangements with Subsidiaries																	
	Approve margin on intra-group loans to/from Subsidiaries on behalf of POL	3.7.8	Must be both						√		√							
	Execute documentation for intra-group loans to/from Subsidiaries on behalf of POL																	
	- up to £20m and up to 3 months	3.7.8	Must be						√									
	- over £20m or over 3 months	3.7.8	Must be		√													
4. MEDIUM AND LONG-TERM FUNDING MANAGEMENT	**Headroom**																	
	Approve amendment to Facility Headroom Buffer	4.8.4	Must be		√													
	Borrowing Policy																	
	Approve new medium and long-term funding	4.9.4	Must be both	√	√													
5. COUNTERPARTY CREDIT RISK MANAGEMENT	**Counterparty Credit Risk Management**																	
	Approve new financial institution counterparty	5.11	Must be			√												
	Approve financial institution counterparty limit	5.11	Must be			√												
	Approve temporary increase to financial institution counterparty limit	5.11	Must be						√									
6. INVESTMENT RISK MANAGEMENT	**Investment Risk Management**																	
	Approve new investment counterparty - within approved credit rating bands	6.14	Any 1 from						√	√								
	Approve changes to credit rating bands for counterparties	6.14	Must be			√												
	Approve temporary increase to investment counterparty deposit limit	6.14	Must be						√									
	Approve new permitted investment instrument	6.14	Must be						√									
	Propose investment of surplus cash balances	6.14	Any 1 from											√				
	Approve investment of surplus cash balances																	
	- Amount - < £300m / Term - up to 1 month	6.14	Any 1 from						√	√	√		√					
	- Amount - < £100m / Term - up to 3 months	6.14	Any 1 from						√	√	√		√					
	- Amount - < £50m / Term - up to 6 months	6.14	Any 1 from						√	√	√		√					
	- Amount - < £300m / Term - up to 1 year	6.14	Any 1 from						√	√								
	- Amount - < £50m / Term - up to 1 year	6.14	Must be both *		√				√									
	- Amount - < £50m / Term - up to 1 year	6.14	Must be		√													
7. FOREIGN EXCHANGE EXPOSURE MANAGEMENT	**Foreign Exchange Exposure Management**																	
	Execute FX hedge trades, within policy, in accordance with instructions issued by FX Committee	7.10	Any 1 from											√				
	Approve new permitted FX hedging instrument	7.10	Must be						√									
	Approve FX hedge trades for exposures not created by currency note inventory holdings																	
	- up to £50m	7.10	Must be						√									
	- above £50m	7.10	Must be		√													
8. INTEREST RATE EXPOSURE MANAGEMENT	**Interest Rate Exposure Management**																	
	Approve new permitted interest rate hedging instrument	8.9	Must be			√												
	Approve execution of interest rate hedging strategy	8.9	Must be		√													
9. BANK RELATIONSHIP MANAGEMENT	**Bank Relationship Management**																	
	Approve entering into relationship with new bank	9.9	Must be				√											
	Approve entering into relationship with new bank - prior to Treasury Committee approval	9.9	Must be						√									
	Approve entering into NDA with bank	9.9	Must be						√									

Data: Confidential

Last Edit: 13/03/2019 12:21
Prepared By: Mark DIXON
Treasury Policy_DA Matrix_03.2019 (ARC)

POL00423454

POST OFFICE LIMITED - Treasury Risk Management Framework, Policies and Authorities
Appendix F - Summary of Delegated Authorities - from March 2019

	Reserved Matter	Ref.	Notes	Shareholder Consent	POL Board	Audit, Risk & Compl. Comm.	Treasury Comm.	FX Currency Hedging Comm.	CFOO	POL FD	Head of Treasury, Tax & Insurance	Treasury Manager	Authorisation Panels: Treasury Authorisation Panel	Dealing Panel	Payment Panels: Banking Auth. Panel	Internet Banking Systems	Treasury Mgt. System	SAP
10. COMMODITY PRICE EXPOSURE MANAGEMENT	**Commodity Price Exposure Management**																	
	Execute commodity price hedges within policy	10.7	Must be											√				
	Approve new commodity price hedge counterparty	10.7	Must be						√									
	Approve execution of commodity price hedges within policy	10.7	Any 1 from						√	√	√							
OTHER	**Operational Banking**																	
	Approve amendments to existing operational banking facilities (2)	11.6	Any 1 from						√									
	Approve new operational banking facilities (2)	11.6	Any 1 from						√									
	Approve opening of new bank account	11.6	Must be						√	√	√							
	Approve closure of bank account	11.6	Must be						√	√	√							
	Payments																	
	Sign manual payment instruction - < £50k	12.1.6	Must be 1 from												√			
	Sign manual payment instruction - < £50k	12.1.6	Must be 2 from												√			
	Release payment from Internet Banking System - < £50k	12.4.7	Must be 1 from													√		
	Release payment from Internet Banking System - > £50k	12.4.7	Must be 2 from													√		
	Release payment from Treasury Management System	12.4.7	Must be Treasury check and 1 from												√			
	Release payment from SAP	12.4.7	Must be 1 from															√
	Guarantees / Group Support																	
	Approve and execute a direct guarantee to a commercial third party for the benefit of a subsidiary (**See Group Delegated Authorities**)	13.1.4	Must be															
	Approve bank guarantee to support financing arrangement	13.2.4	Must be		√													
	Approve bank guarantee to support commercial arrangement (**See Group Delegated Authorities**)	13.2.4	Must be															
	Execute counter-guarantee to bank in support of commercial arrangement (**See Group Delegated Authorities**)	13.2.4	Must be															
	ISDA Master Agreements																	
	Agree changes to an ISDA Schedule	15.4	Any 1 from						√	√	√							
	Approve and execute ISDA agreement on behalf of POL	15.4	Must be						√									

** Must be CFOO and one other POL Board member*

(1) unless specifically stated as the Board (2) including overdrafts, fax lines, BACS limits, intra-day limits and similar arrangements