POL00423464

Audit, Risk and Compliance Committee Agenda

Date:	Monday 23 September 2019	Time	08.00 – 10.30 hrs	Location	1.19 Wakefield

Present	Other Attendees	
• Carla Stent (Chair) • Tom Cooper • Tim Franklin • Ken McCall **Apology:**	• Nick Read (CEO) • Alisdair Cameron (CFO) • Tim Parker (Chairman – PO Limited) • Ben Foat (General Counsel) • Andrew Paynter (Audit Partner, PwC) • Rosie Clifton (Audit Manager, PwC) • Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Jonathan Hill (Compliance Director) • Micheal Passmore (Finance Director) • David Parry (Senior Assistant Company Secretary) • Amanda Bowe (item 2.) – by telephone (Chair, ARC PO Insurance Director) • Ben Cooke (item 4.) (IT Operations Director)	• Shikha Hornsey (item 5.) (Group CIO) • Tony Jowett (item 5.) (Chief Information Security Officer) • Phey Rasulian (item 5.) (Programme Manager Payment Services, Retail) • Dan Zinner (item 6.) – by telephone (Chief Transformation Officer) • Mark Dixon (item 8.) (Head of Treasury, Tax & Insurance) • Andy Bear (item 8.) (Account Manager, Locktons) • Amanda Jones (items 10, 11, 12) (Retail Director) • James Scutt (item 10) (Head of Customer Experience, Retail) • Andrew Kingham (item 11) (Sales Capability Manager) • Karl Oliver (item 12) (Head of Commercial Partnerships, Retail) • Tom Lee (item 13) • (Head of Finance, Financial Accounting and Controls) • Christine Kirby (item 13) (Financial Controls Manager)

	Agenda Item	Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest**	Noting	Chair	08.00 – 08.05
2.	**Update from Subsidiaries:** • Post Office Management Services ARC	Noting & Input	Amanda Bowe	08.05 – 08.10
3. 3.1 3.2 3.3 3.4	**Minutes and Matters Arising** Minutes of the Audit, Risk and Compliance meeting held on 23 July 2019 Minutes of the Audit, Risk and Compliance meeting held on 29 July 2019 Actions List Draft Minutes of the Risk and Compliance Committee held on 3 September 2019	Approval Noting & Input Noting	Chair	08.10 – 08.15
4.	**Belfast Data Centre Disaster Recovery lessons learned**	Noting & Input	Ben Cooke	08.15 – 08.35

POL00423464

Audit, Risk and Compliance Committee Agenda

5.	**PCI-DSS Update and Cyber Security Update** Includes Cyber Risk Appetite	Noting	Shikha Hornsey/ Phey Rasulian/ Tony Jowett	08.35 – 08.50
6.	**Transformation Office Changes**	Noting & Approval	Dan Zinner	08.50 – 09.00
7.	**Consolidated Report from Risk, Compliance and Internal Audit**	Noting & Input		09.00 – 09.30
7.1	Risk Report		Jenny Ellwood	09.00 – 09.10
7.2	Compliance Report		Jonathan Hill	09.10 – 09.20
7.3	Internal Audit Report		Johann Appel	09.20 – 09.30
8.	**Corporate Insurance Renewal**	Noting & Input	Mark Dixon/ Andy Bear	09.30 – 09.40
9.	**Policies for Approval – Policies are in the reading room.** • Contract Execution • Financial Crime • Anti-Money Laundering and Counter Terrorist Financing includes the HMRC Fit & Proper Standards Policy • Physical Security • Vulnerable Customer	Approval		09.40 – 09.45
10.	**Modern Slavery Statement**	Approval	Amanda Jones/ James Scutt	09.45 – 09.55
11.	**Deep Dive: FS Quality of Sales in the Network**	Noting & Input	Amanda Jones/ Andrew Kingham	09.55 – 10.05
12.	**Deep-Dive: Monitoring of Multiple Retail Partners**	Noting & Input	Amanda Jones/ Karl Oliver	10.05 – 10.15
13.	**Deep-Dive: Financial Controls**	Noting & Input	Micheal Passmore/ Tom Lee/ Christine Kirby	10.15 – 10.25
14.	**Provision of External Auditor Consulting Services**	Noting & Approval	Micheal Passmore	10.25 – 10.30
15.	**Any other Business** Notes: • Date of next meeting 25 November 2019, 16.00 – 18.00 hrs. • Nigel Boardman (BEIS ARC Chairman) will be observing the next ARC meeting of 25 November 2019. • NEDs meet IA at the next ARC meeting of 25 November 2019.	Noting	Chair	10.30 – 10.30

POL00423464

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 23 JULY 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 09.00 AM IN PERSON AND BY TELEPHONE

Present:	Carla Stent	Chair **(CS)**
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)** (by telephone)
In Attendance:	Alisdair Cameron	Interim CEO (**AC**)
	Kathryn Sherratt	Interim CFO (**KS**)
	Micheal Passmore	Finance Director (**MP**)
	Tom Lee	Head of Finance, Financial Accounting and Controls (**TL**)
	Deana Hurley	Head of Risk, Governance and Assurance (**DH**)
	Andrew Paynter	Group Audit Partner, PwC **(AP)** (by telephone)
	Lucy Mason	Group Audit Senior Manager, PwC **(LM)** (by telephone)
	David Parry	Senior Assistant Company Secretary (**DP**)
Apologies:	Tim Franklin	Non-Executive Director

ACTION

1. WELCOME AND CONFLICTS OF INTEREST

1.1 The Chair welcomed everyone to the meeting and explained that the purpose of the meeting was to review the figures for the 2018/2019 Annual Report and Accounts and to discuss any findings from PwC's audit.

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. ANNUAL REPORT AND ACCOUNTS EXTERNAL AUDIT 2018-2019 (ARA)

2.1 CS sought and received confirmation from AC that the audit work was almost complete, and, barring minor outstanding audit work, he believed that the numbers presented could be signed off today. GLO disclosures would not be discussed in this meeting but would be reviewed in more detail at next week's ARC meeting of 29 July.

2.2 A final read through of the ARA was planned for this week, with sign off planned at the end of next week (w/c 29 July) and publication when Parliament was convened again in September.

2.3 Whilst he did not believe that the business was able to make a reliable estimate of any liability in connection with the GLO, the disclosures had not been finalised. In response to a question on the timings of the verdicts, AC stated that he believed that this might only have an impact if the verdicts are not in POL's favour and if Parliament could not be re convened in September (eg if a general election was called before September).

2.4 It was further noted that the Group financial numbers presented would inform the decision regarding management bonuses to be considered at next week's Remuneration Committee meeting.

2.5 AP echoed AC's comments that the audit was near completion and, apart from some minor outstanding points not believed to be significant, he was comfortable with the numbers presented. The paper PwC had tabled, covered the key areas of audit focus since that last ARC update in May.

2.6 **Impairment of tangible and intangible assets**

AP noted the group headroom figure of IRRELEVANT and advised that he was comfortable with the judgements presented. To avoid the risk of the carrying value of intangible assets being obsolete or superseded, a review of each intangible asset was completed by management to ensure that the

POL00423464

carrying value of the asset continued to be supported. Whilst all numbers and judgements were sound, AP recommended that this should be kept under review.

2.7 **Lease provision**

An updated model had identified that a number of branches required removal from the provision and some needed adding, resulting in a net increase of fourteen branches within the onerous provision. In line with IAS37, costs allocated to branches had been reviewed by management with no issues identified but would be kept under review.

2.8 **IFRS 16**

AP reported on a new accounting standard, IFRS 16, which would be effective for POL's 2019/20 year end. Lessees will be required to recognise the lease liability (which reflects future lease payments) and a 'right-of-use' asset ie the lease values will be reflected in the balance sheet. He noted that management had applied a retrospective transition approach to implement IFRS 16 and was happy with the judgements that had been applied.

2.9 **Pension scheme liabilities**

AP noted POL has two defined benefit schemes: the POL fund of the Royal Mail Pension Plan (RMPP) and the Post Office Limited's share of the Royal Mail Senior Executive Pension Plan (RMSEPP).

2.10 He noted the plan was in surplus and whilst he was comfortable that this surplus was not recognised in the balance sheet, verification was required over the 7% allocation of assets and liabilities to the Post Office RMSEPP pension scheme. Historically, pension assets have been split 93%/7% between the two pension schemes, and whilst monitoring has been infrequent, the 7% is supported by the percentage contributions made to the fund.

2.11 **Classification and recognition of Investments**

Unlike comparable listed companies, AP noted that POL used a two column format for the ARA approach for the income statement (and a three column format for budgeting). This was to segregate the results of the 'business as usual' activities from net income and expenditure associated with business transformation activities and associated government funding.

2.12 KM raised one concern that revenue costs for the Bank of Ireland, although a trading item, was treated as a bridging item and questioned why this was not built into the budget. CS replied that the Board had approved the treatment of revenue for the Bank of Ireland as an exceptional cost and was cognisant of this fact.

2.13 The Committee discussed the approach and AC and CS both confirmed that the approach had been approved by the Board and could be considered satisfactory. Funding tied to particular projects had to be clearly identified as such.

2.14 TC confirmed he was happy with the presentation as the layout was clear and made sense. The Committee agreed to continue reporting in this manner through to the end of the current, agreed investment funding cycle.

2.15 TC sought and received confirmation that the IRRELEVANT million adjustment to the financial statements of POMS related to BGL trading. AC reported that treatment advice differed between the current and former auditors.

2.16 Regarding the re allocation of cash transactions to accounts receivable, TL reported that this would continue to be monitored and that a large manual exercise had been completed to reconcile differences that had arisen as a result of the Back Office Transformation (specifically, cash centres had moved to a new system called CWC). AC assured the Committee that there will be no further issues arising in the subsequent financial year, once the remaining CWC issues are resolved.

2.17 Regarding user access for previous agents, some work was still required to rectify this. AC confirmed that an update would be presented to the ARC in the Autumn.

POL00423464

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

2.18 The Chair sought and received confirmation that the Committee was satisfied with the numbers presented and confirmed that they could be used as a basis for the Remuneration Committee discussion next week.

2.19 The Chair thanked the finance team and the auditors for all their work. AC echoed these comments.

The meeting closed at 09.45 am.

…… ……

Chairman **Date**

POL00423464

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

3.2

MINUTES OF A MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON MONDAY 29 JULY 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 14.30 PM

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:	Alisdair Cameron	Interim CEO **(AC)**
	Tim Parker	Chairman, PO Limited **(TP)**
	Andrew Paynter	Group Audit Partner, PwC **(AP)**
	Lucy Mason	Group Audit Senior Manager, PwC **(LM)**
	Ben Foat	General Counsel **(BF)**
	Charlotte Webster	Internal Audit Manager **(CW)** deputising for Johann Appel
	Jenny Ellwood	Risk Director **(JE)**
	Jonathan Hill	Compliance Director **(JH)**
	David Parry	Senior Assistant Company Secretary **(DP)**
	Rob Houghton	Group Chief Information Officer (item 4)
	Mark Fabes	Interim Group CIO (MF) (item 4.1)
	Phey Rasulian	Programme Manager Payment Services, Retail (PR) (item 4.1)
	Tony Jowett	Chief Information Security Officer (item 4.2)
	Ben Cooke	CIO Back Office (items 7, 8)
	Tim Armit	Business Continuity Manager (items 8, 9)

Apologies:

Action

1. Welcome and Conflicts of Interest

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

2. Update from Subsidiaries

TF provided an overview of the key issues discussed at recent Post Office Insurance (POI) Audit and Risk Committee meeting of 18 July:

- POI Accounts for the year end 2018/19 are being finalised pending a small number of outstanding audit deliverables. There are no items of concern and POI Board is expected to approve these by 31 July 2019.
- The auditors have flagged a recurring issue of ineffective controls regarding the removal of leavers from IT systems. Further work on control remediation is required to ensure this is managed more effectively going forward.
- POI Board has re-approved the appointment of PwC as External Auditors.
- Good progress has been made closing Internal Audit actions within period.
- Updates from Sally Smith on Anti-Money Laundering, Anti-Bribery and Corruption, Countering Financing on Terrorism and Whistleblowing were received. It was agreed POL ARC would receive an overview of the annual POI MLRO report.
- A deep-dive on Complaints was received looking at data, identifying emerging trends and reviewing the effectiveness of current policies/processes.
- The quality of branch sales and disappointing mystery shopping results remain a concern.
- ERV has now been successfully established as underwriter replacing TIF.

POL00423464

- Brexit remains a key risk with a 'hard' exit on 31 October 2019 now a significant risk. Existing mitigation plans are in place and will be refreshed for review in September.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 29th May 2019 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

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

3.3 The draft minutes of the Risk and Compliance Committee held on 4 July 2019 was **NOTED**.

4. PCI-DSS Update and Cyber Security Update

4.1 **PCI DSS**

The paper was taken as read.

PR and MF presented an update on current status.

Following senior level talks held in June with Ingencio, engagement had now been brought forward by one month and workshops to review the detailed design and to refine the delivery plan were underway. A high level plan expected at the end of next week would be circulated to the Committee.

Action: MF/PR

MF remarked that the team was investigating the possibility of alternative solutions to manage both retail and banking transactions under one single solution. Unlike banks, POL completed both retail and banking transactions which made it unique to the market place. Further, Ingencio had limited experience when dealing with banking transactions.

KM sought and received confirmation that the level of risk was being managed effectively. The banks received monthly updates on PCI compliance and had been informed that full compliance was expected to be achieved between Q2 – Q4 2020.

Following a query from TC on the processes/products that were not PCI compliant, PR explained that an operating model workstream was analysing these and that a holistic approach had been taken requesting providers modify their processes/products to be compliant.

In terms of the risk to POL not being PCI compliant, TJ advised the biggest risk was reputational, however he believed POL's security was effective against attack and that the team was vigilant to any threats.

The Committee requested the project be kept on track to avoid further delay.

4.2 **Cyber Security**

The paper was taken as read.

TJ noted the recent regulator fines for data protection breaches in the UK and America, and stated that the team was proactively assessing whether any lessons could be learnt. A cyber threat intelligence provider (Recorded Futures) had been on-boarded which ensured closer liaison with the National Cyber Security Centre.

Good progress had been made to implement the recommendations from Deloitte's audit on IT and Cyber security, however implementation of RSA Archer for the Security Operation enhancements (SOC) was behind schedule due to internal organisational changes. The team was still aiming to complete implementation of RSA Archer by January 2020 and Deloitte's recommendations by March 2020.

Security reviews have commenced with third party suppliers to ensure that suppliers are governing themselves in line with POL's Cyber Security policy and standards. KM requested that outstanding questionnaires be followed up with suppliers and that a plan be established to deal with third party governance highlighting the key risks to POL.

The Committee discussed and noted TJ's current concerns with third party providers and questioned whether audits of these suppliers should be completed. RH noted an audit of Computacentre had been completed, but that the recommendations had not been tested to date.

Regarding maturity scores against Deloitte's Maturity Review, POL had focused on the categories that had the worst rag ratings and the largest maturity gap. Following a query from TC on how current the data was, TJ explained the maturity scores represented data taken from Deloitte's client base in 2018 and refreshed annually.

RH, PR, TF & TJ left the meeting.

5. Annual Report and Accounts – Audit update and GLO and Starling disclosures

5.1 **Audit**

The paper was taken as read.

AP remarked that the audit was on the last straight with sign off this Thursday (1 August). He was comfortable with the numbers presented and noted the approach regarding the GLO disclosure had been endorsed by PwC Technical Partner – to be treated as a contingent liability.

Talks are still in the early stages and the outcome at present is unknown.

5.2 **Starling disclosure**

BF explained the Starling disclosure related to a claim from 123 Postmasters to determine whether they were considered to be workers of POL and if so, whether they would be entitled to unpaid holiday pay.

[redacted]

The Committee noted the disclosure.

5.3 **GLO disclosure**

Regarding the GLO disclosure, BF explained this claim related to 555 claims being heard against POL currently over a series of at least four trials.

AC commented that in view of the judgement from the common issues trial (the first trial), POL's new strategy was to consider alternative dispute resolution through mediation. This meant that an economic outflow within this financial year was possible, however, a sensible number could not be provided because:

- POL was unaware of the claimants expectations for settlement or whether they are prepared to settle; and

POL00423464

- the claim valuation is unreliable.

KM questioned whether POL could have foreseen this happening and questioned whether it was sensible not to include a set of costs.

The Committee noted that the reasonableness test had been passed and that under IAS 37, a provision should only be made when the following criteria had been met:

a. an entity has a present obligation (legal or constructive) as a result of a past event;
b. it is probable that an outflow of resources embodying economic benefits will be required to settle the obligation; **and**
c. a reliable estimate can be made of the amount of the obligation.

However, POL had:

a. no present obligation;
b. a probable outflow but no reasonable assumption could be provided; **and**
c. a robust defence.

AP remarked that whilst the regulator could question why provision had not been made, he recognised that POL was unaware of the claimant's expectations for settlement and that mediation was under consideration.

The Committee discussed whether it would be appropriate to include a statement on the Criminal Cases Review Commission (CCRC) cases within the disclosure. In view of making a full and transparent disclosure and of being true and fair, the Committee **AGREED** that a separate sentence should be included within the GLO disclosure. **Action: BF**

The Committee noted the disclosure.

Following a discussion of the disclosures and audit progress made, the Committee **RECOMMENDED** that the Annual Report and Accounts for 2018/19 be submitted to the POL Board for approval.

It was noted the GLO and Starling disclosures would be discussed in further detail at the next POL Board meeting.

The Chair thanked the auditors and the financial team for all their hard work.

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

6.1 **Risk**

The report was taken as read.

JE presented an update on POL's current risk profile.

She remarked that there had been no significant change to POL's risk profile with continued focus on Litigation, Change Portfolio, PCI-Compliance, Brexit and Key personnel changes all remaining 'red'.

GLO Litigation

The findings/outcomes from the second trial are expected in early September. Deloitte are assisting the team with workshops to record risks, mitigations and to allocate owners.

Change Portfolio

POL00423464

The Change portfolio remains at 'Amber' and a new transformation director has been appointed to expedite the change process as it is apparent that some changes are not at the required/expected level of change.

PCI Compliance

PCI continues to report as 'Red' with no significant progress being made since last year.

Brexit

Dialogue continues on a fortnightly basis with BEIS regarding a 'No Deal' Brexit on 31 October 2019. Remediation work on a 'No Deal' is ongoing particularly POL's engagement with third parties who are yet to respond to POL's questionnaire. However it was noted that all key partners have been contacted and services will remain the same.

JE remarked the Operations Working Group would be re-established to review the original contingency plans and to agree any new actions. Consideration was being given to IT and Marketing releases and to cash supply and distribution. Overtime will be sanctioned to ensure cash centres can manage any upsurge.

Branches would be closed should there be any security issues and electricity supply to Northern Ireland branches would be provided by companies from both Northern Ireland and the Republic.

KM sought and received confirmation that JE had been liaising with industry contacts and AC noted the possibility of civil unrest in October.

Key personnel changes

In view of key personnel changes at senior positions, the review and assessment of the capability of senior positions continued, along with a review of career progression to understand current and future requirements for talent development.

Payzone

Remediation work following the Payzone penetration testing remains ongoing and is on track, with all security vulnerabilities expected to be resolved by October. A Payzone risk workshop is planned for 30 July 2019 to help develop Payzone's risk management framework and governance.

TF commented that it would be useful to understand the levels of engagement POL had with Deloitte and PwC, and to confirm whether there were any conflicts of interest or Chinese walls to be aware of.

6.2 Compliance

The report was taken as read.

JH highlighted the following key compliance issues:

Text Relay
Ofcom had requested further information to evidence when senior managers were informed of non-compliance, which the team was collating. He believed the regulator was becoming more stringent than before, and a provision of IRRELEVANT had been set aside to cover a potential fine.

GDPR
The GDPR project was formally closed at the end of Q1 and compulsory data protection training had gone live for all employees.

POL00423464

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

TC noted that there are a number of projects that would assist with GDPR compliance and remarked that contract remediation was a large job to undertake. JH reported that this was currently being reviewed and that a progress report would be discussed at the Risk and Compliance Committee meeting.

Privacy and Electronic Communications Regulations notifications

CS sought further information on the two Privacy and Electronic Communications Regulations notifications. JH remarked these were as a result of error in the Telecoms centre. Training had been reviewed and refreshed, however he assured the Committee this was not a systematic issue.

Fit & Proper

The team remained focused on gathering agent returns and data was shared with HMRC on fortnightly basis to evidence progress. It was noted the regulator had agreed to extend the deadline until September. Returns from four commercial partners remained outstanding along with 1162 outstanding responses from non-commercial partners.

Despite repeated warnings to commercial partners and agents, the Committee sought and received assurance that a strong stance would be taken to switch off Partners/Agents Travel Money and MoneyGram services on 30 August 2019 should their returns not be completed by 23 August 2019.

Compliance with Money Laundering Regulations
TC noted the large number of Bureau de Change non-conformance cases (66 identified between 24 April and 19 June 2019) where customers had purchased in excess of €15k in 90 days and sought to understand who the culprits were.

JH replied that this was under investigation but that this information could not be divulged for confidentiality reasons.

Mystery Shopping
TF sought and received confirmation that mystery shoppers do not identify what was said by agents in their reports. Results have declined since April which JC explained could be attributed to the re-structure and re-focus of the Area Manager teams, with less time given towards supporting client relationship managers who were on the front line.

The Committee noted and discussed the decline in mystery shopping standards and requested that Amanda Jones be invited to discuss the FS quality of sales in the network at the next ARC meeting in September.

Further, it was felt that senior level staff should be held more accountable for declining standards.

5th Money Laundering Directive
JC advised that the 5th Money Laundering Directive would be adopted in the UK coming into force in January 2020. The directive set about tighter regulations regarding money laundering, due diligence and ownership and control of companies and a requirement to list politically exposed persons.

POL00423464

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

6.3 Internal Audit

The report was taken as read.

CW, deputising for Johann Appel, was welcomed to the meeting.

She reported that eight reviews had been finalised since the last ARC meeting and good progress had been made with the 2019/20 Internal Audit plan. 24 of the 26 audits for 2018/19 had been completed with the two outstanding audits on assurance being included under the change audit in the 2019/20 plan.

The Committee discussed and noted the recurring key themes and root causes of audit actions reported in 2018.2019. These included change delivery, control activities, information & communication and risk assessment.

KM noted that the average time to clear internal audit report was still higher than the agreed target. AC provided assurance that governance and turnaround had improved with formal closure meetings for each audit with the GE sponsor and management executive and a clear escalation process to prevent significant delay. The Committee acknowledged that standards had improved.

TC requested the Payzone Master Services Agreement be completed to avoid any future risks.

7. Transtrack

The paper was taken as read.

BC and TA entered the meeting.

BC presented an update on IRRELEVANT

IRRELEVANT

8. Belfast Data Centre Disaster Recovery testing

The paper was taken as read.

BC explained the centre (operated by Fujitsu) hosted POL's Horizon, counter trading application and other business critical applications and that resilience had not been tested since 2013.

The team planned to carry out a test exercise over the August Bank holiday weekend when trading was significantly lower than usual trading days, whilst noting that the bank holiday Monday is a normal trading day in Scotland.

POL00423464

He advised the primary system would be switched off on Saturday evening to the back-up system, so Sunday trading would be on the back-up system. On Sunday evening, the team would revert to the primary system ready for Monday trading in Scotland.

The team was technically confident the exercise would be a success and remarked that a workshop had been recently held to run through the risks and mitigating actions.

TA remarked that there is little contingent processes in place to manage a full loss of Horizon. Whilst there was no optimum time in which to test the centre's resilience, the team recognised the close proximity to the publication of the judgements from the second trial and the reputational risk to POL of the Horizon system not working.

The Committee wished the team good luck.

BC left the meeting.

9. Business Continuity Update and Policy

9.1 The paper was taken as read.

TA advised that business continuity was now established in POL and had moved from development to business as usual and was pleased with the progress made to date.

A system had been implemented to communicate to all branches when Horizon failed and Business Continuity recovery strategies are now in place and tested for all locations. Resilience in building design is being improved across all key locations and regular evacuation testing takes place across all sites.

KM noted the improved changes but advised that he was alarmed with the volume of red rag ratings in the risk appetite paper which suggested a live risk.

TA assured the Committee this was not the case and that many of the red items were only red because 3rd party plans had not yet been evidenced and validated. Action plans including mitigating actions and deadline dates would be included in the risk appetite to allay any fears.

To do: TA

TA left the meeting.

9.2 Business Continuity Policy

The ARC **APPROVED** the Business Continuity Policy.

10. Change Update

The Chair advised the paper would be removed from the agenda to be reviewed at a later date. The paper had not been discussed at the Risk and Compliance Committee meeting.

11. GDPR

The paper was taken as read.

JH explained the programme was formally closed at the end of Q1 with controls established to ensure the POL was operationally compliant.

Further work is required on contract remediation, records retention, data classification and data storage to enhance POL's ability to evidence that effective compliance has been achieved. Additionally, a 'Privacy forum' is being proposed to meet quarterly to support the business manage data compliantly with oversight provided by the data protection team.

Action:

POL00423464

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

CS queried the number of "right to be forgotten" requests. JH advised he would investigate this and revert accordingly. **JH**

It was agreed that GDPR would be reported on a 6 monthly cycle until further notice.

12. AOB

The following policies were reviewed by the Committee:

- **Modern Slavery Statement** – it was agreed the statement should be re-reviewed at a later date as it was unclear whether progress had been made. The Committee required examples of what had been completed at a practical level to provide assurance that the actions had been completed.
- **Anti-Bribery and Corruption Update and Policy** – the Committee noted the update and **APPROVED** the policy.
- **Whistleblowing Policy** - the Committee noted the update and **APPROVED** the policy.

There being no further business, the meeting closed.

.....
Chairman Date

Actions from meeting

Minute	Action	Lead	Due Date
4.1	**PCI-DSS** – circulate high level plan to the ARC following Ingencio workshops on detailed design and the refined delivery plan.	MF/PR	ASAP
5.3	**ARA 2018/2019** – to include a sentence/comment on the Criminal Cases Review Commission cases in the GLO disclosure.	BF	ASAP
11	**GDPR** – to confirm the number of "right to be forgotten" requests.	BF	Sept

POL00423464

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
30 October 2018					
11. Insurance Policies	Review the risks covered by the suite of Insurance policies.	**Jenny Ellwood**	~~May 2019~~ ~~July 2019~~ September 2019	~~Update to be given at the May ARC meeting. Following discussion with the Chair, an update will be provided in the July ARC meeting.~~ An update will be provided at the September ARC meeting.	Open
29 January 2019					
2. (b)	ARC to review the quality of sales of financial services products in the branch network in more depth.	**Jonathan Hill**	~~May 2019~~ July 2019	~~Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.~~ A deep dive is being presented in September.	Recommend for closure
6. Money Laundering Reporting Officer (MLRO) Annual Report					
6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	**Nick Boden/ Sally Smith**	Ongoing	**Ongoing until project close.** Item included on ARC agenda.	Open
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	**Rob Houghton / Mick Mitchell**	May 2019	**Ongoing.** Item included on ARC forward agenda.	Open
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	**Exec**	~~May 2019~~ July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open
29 July 2019					
4. PCI-DSS and Cyber Security Update					
4.1 PCI-DSS	Circulate high level plan of the detailed design and refined delivery plan.	**Rob Houghton/ Phey Rasulian**	July 2019	Plan circulated to ARC 05/08/2019.	Recommended for closure
5. Annual Report and Accounts 2018/2019					
5.3 GLO Disclosure	A separate sentence to be included in the GLO disclosure on the Criminal Cases Review Commission (CCRC) cases.	**Ben Foat**	July 2019	Separate sentence included in the GLO disclosure.	Recommended for closure
11. GDPR Update					
11. GDPR	CS queried the number of "right to be forgotten" requests. JH advised he would investigate this and revert accordingly.	**Jonathan Hill**	July 2019	An update has been provided in Appendix 7 of the reading room.	Recommended for closure

POL00423464

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 22.07.19

POL00423464

3.4

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 4 July 2019 at 13.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Interim Chief Executive Officer
	Shikha Hornsey (SH)	Group Chief Information Officer
	Mo Kang (MK)	Group HR Director
	Debbie Smith (DS)	Chief Executive Officer, Retail
	Owen Woodley (OW)	Chief Executive Officer, Financial Services, Telecoms and Identity, Group Marketing and Group Digital & Innovation
In Attendance:	David Parry (DP)	Senior Assistant Company Secretary
	Garry Hooton (GH)	Internal Audit Manager (deputising for Johann Appel)
	Jenny Ellwood (JE)	Risk Director
	Jonathan Hill (JH)	Compliance Director
	Phey Rasulian	Programme Manager Payment Services, Retail (items 3 & 4)
	Tony Jowett (TJ)	Chief Information Security Officer (items 3 & 4)
	Dan Zinner	Chief Transformation Officer (item 6)
	Barbara Brannon (BB)	Purchasing Director (item 7)
	Amanda Jones (AB)	Retail Director (items 8.6, 9 & 10)
	James Scutt (JS)	Head of Customer Experience, Retail (item 8.6)
	Andrew Kingham (AK)	Sales Capability Manager, Retail (item 9)
	Karl Oliver (KO)	Head of Commercial Partnerships, Retail (item 10)
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls (item 11)
	Christine Kirby (CK)	Financial Controls Manager (item 11)
Apologies	Ben Foat, General Counsel; Johann Appel, Head of Internal Audit	

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

1.1 AC opened the meeting.

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

2. Minutes and Action Lists

2.1 The minutes of the RCC meeting held 4 July were **APPROVED**.

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

3. PCI-DSS Update

3.1 The paper was taken as read.

3.2 AC questioned the levels of progress made since the last meeting and noted that no definitive action plan regarding the banking solution had been committed to.

3.2 PR reported that a detailed design plan (regarding the banking solution) was expected by the end of October. Following stringent conversations between Ingenico and Mark Fabes (Interim Group CIO), recruitment of additional resources to help increase the speed of delivery is underway. Furthermore,

POL00423464

Ingenico had been advised that their priority was to ensure delivery of PCI compliance before December 2020 and not beyond.

3.3 Regarding the alternative banking solutions under investigation (to provide an outsourced capability that could process both retail and banking transactions), early findings from the feasibility study had indicated that there was no significant differentiator that indicated POL would receive a solution quicker or at a reduced cost. Analysis continues. The findings from the feasibility study were expected at the end of this month.

3.4 JE questioned the benefits of postponing the roll-out of the pin-pad devices across the Milton Keynes branches. PR advised that this would not impact the overall timeline as the pin pad rollout was not on the critical path. The pausing of the roll out activities provided an opportunity for POL to explore the alternative providers (FIS Global and ACI) and understand if those same activities were required should POL choose an alternative solution.

3.5 The Committee discussed the capability of the pin-pad devices and noted that a decision had previously been made to use a single pin-pad device for both retail and banking transactions. This had meant compliance would take longer to complete. SH reported that as retail can have its own solution, PCI compliance for Retail alone could have been met sooner; however it was felt the expenditure for two separate devices could not be justified.

3.6 AC requested the following changes be made to the paper: To do: PR

1. Explain that POL is not PCI compliant.
2. Explain that POL could be compliant in retail but is not.
3. Highlight the findings from the feasibility study that Ingenico remains the preferred solution and why the alternative solutions are not a creditable.
4. Highlight spend to date and in future.
5. Set out risks.
6. That POL's plans are supported by third parties.

He further wished to understand why the banks were happy for POL to be non-compliant.

4. Cyber Security

4.1 The paper was taken as read.

4.2 AC sought an update on the progress levels made with the Deloitte recommendations.

4.3 TJ reported good progress had been made with eight of the 10 recommendations being completed and he expected a ninth recommendation to be completed in September. Target maturity remained on track for March 2020 although it was noted that there was still a large amount of work required to do. IRRELEVANT IRRELEVANT s that POL would not have previously been aware of and the security operations centre (SOC), had been central in responding to a large number of incidents across the estate.

4.4 Regarding the data breach experienced by Capital One in the USA (Capital One provide credit cards to POL customers), TJ reported that he had met with Capital One's Chief Information Security Officer to seek assurance that no POL customers had been impacted and to clarify the nature of the hack. There was no impact to POL or POL's customers.

4.5 AC commented on the varying levels of disaster recovery testing in place across all suppliers (as mentione d in the Business Continuity paper presented at the last RCC meeting) and sought to understand whether responses had been received from suppliers. TJ replied that responses from the main suppliers were under review and that the team would continue to chase those outstanding.

POL00423464

4.6 *Cyber Security Risk Appetite*
The Committee noted the risk appetite statements had not been reviewed or refreshed since 2015 and did not accurately reflect the current threat landscape. However it was noted that no alternative realistic approach could be taken.

4.7 A review of the statements was undertaken to align them with the current threat landscape. This had resulted in the following: To do: TJ

- A new proposed cyber risk/data security statement that set out expectations for data protection and importantly did not require all data to be managed with an 'averse' appetite.
- A new risk approach to operationalise the Board's appetite statements using the existing Document Classification Standards and a simple Confidentiality, Integrity and Availability score.
- A simpler method for managers to assess the risks faced against an agreed Likelihood and Impact score using POL's revised harm table and heat map.
- A faster and more accurate identification of where a risk might be 'outside appetite' and requires further mitigation and identification of when a risk requires escalation.

4.8 The Chair requested the risk appetite paper be integrated into the cyber security paper.

5. Combined Risk, Compliance and Audit Update

5.1 **Risk**

5.2 The paper was taken as read.

5.3 JE reported that the top risks to POL included PCI compliance, Information Security, IT Technology, Interruption and Brexit. A watching brief remained on Fit & Proper and the Banking Framework risks. The following items from the paper were raised by the Chair.

5.4 *PCI Compliance*
PCI continued to report red. Ingenico had not provided a definitive plan regarding the banking solution and challenge remained with the timeline and costs of the new schedule. The Chair requested that care should be taken to ensure the PCI-DSS update and risk update were aligned.

5.5 *Ofcom text relay investigation*
The Chair noted the potential fine from Ofcom for non-compliance regarding overcharging vulnerable customers. He requested that further information be included in the risk report including the mitigating actions taken to date. He did not believe the risk should be considered as "significant".

5.6 *Operator Self-funding (OSF) branch insolvency*
The Chair noted that an OSF branch declared insolvent had resulted in a £400k loss. He requested further details be provided on this incident, plus a broader picture on the fraud risks faced by OSF branches and their future.

5.7 *Intragroup agreement*
The Chair sought to understand whether the intragroup agreement had been signed. DS advised she would liaise with BF.

5.8 *Fit & Proper*
The Chair requested the current position be presented in the paper.

5.9 *Succession planning and talent acquisition*
The Chair noted plans had been presented to the Board regarding succession planning and talent acquisition. Reviews of bench strength was ongoing. A debate would be held by GE later in the year.

5.10 *Horizon Integration Hub (HIH)*

The Chair noted that as part of POL's IT strategy of developing solutions optimising the use of cloud technology, HIH had been migrated to Microsfot Azure.

5.11 **Compliance**

5.12 The paper was taken as read. The following points were discussed.

5.13 *Text Relay*
POL provided a response to the second part of Ofcom's investigation on 21 June, with an extension granted until 12 September to allow for the review and identification of documents and emails in scope. JH noted he and Meredith Sharples (Telecom Director) were due to meet with Ofcom.

5.14 *GDPR*
JH reported that 93 contracts required remediation and that a working group had been established to review remediation. The majority of contracts requiring remediation were IT Service contracts where no contract owner had been identified.

The Chair requested a co-ordinated effort be made to identify owners. **Action: SH/BB**

5.15 *Compliance with Money Laundering Regulations*
It was noted that 91 new Bureau de Change non-conformance cases had been identified between 20 June and 14 August 2019, with 98 open cases resolved during that period. JH assured the committee that there was not a problem with money laundering and that the team was on -top of all cases.

5.16 *Fit & Proper*
The team remains focused on gathering F&P returns, with fortnightly updates being provided to HMRC. The Declaration Oversight Committee had met recently (28 August) to formally approve switch off of non-compliant branches and impacted branches would be notified.

5.17 The Chair requested current data be walked in to the ARC.

5.18 *External Threats*
The Committee noted the growing number of high value complex ca ses related to banking deposits where money derived from criminal activity had been placed over POL counters. HMRC had highlighted three cases (totalling £22m) to the UK's Joint Money Laundering Intelligence Taskforce. JH remarked this related to gang activity rather than to three individuals per se.

5.19 *Vulnerable Customers*
JH highlighted that Ladbrokes Coral had recently been fined £5.9M by The Gambling Commission for not protecting vulnerable customers and for failing their anti-money laundering measures. POL sold limited gambling products, but recognised the importance of protecting vulnerable customers.

5.20 **Internal Audit**

5.21 The paper was taken as read.

5.22 No new IA reports had been issued since July, however the following seven audits are in progress:

- Procure to Pay
- Data Analytics Excellence (Change)
- Effectiveness of Gating Ph1 (Change)
- Effectiveness of Second Line Assurance Ph1 (Change)
- Benefits Realisation Ph1 (change)
- SGEI Reporting
- Employee Expenses Follow-up

To do:

It was noted four overdue actions related to Payzone required completion. DS advised she would chase these up. **DS/BF**

6. Change Update

6.1 The paper was taken as read.

6.2 DZ reported that the new centralised Change programme ways of working was not yet fully embedded into POL and that the programme was still working to improve maturity possibly due to: confusion over the changes being made; the lack of appropriate resource in place; and the desire to be "best in class" quickly without resolving underlying capability issues. Immediate focus for the ways of working in the Change programme was on delivery through three key themes: "people", "process" and "perception".

6.3 "People" covered having the appropriate resources, and properly configured teams, in place to deliver, communicate and effectively deliver change. "Process" covered the embedding of consistent Change management and clear reporting lines; having a centralised reporting source on Change; and creating consistent information dashboards that kept all stakeholders actively engaged and updated on progress and to mitigate any risks. "Perception covered ensuring the business understood, was convicted to, and aligned with change.

6.4 The Chair noted DZ's comments that he was in the process of recruiting additional resource (with the appropriate skills and expertise) to accelerate the programmes' status. The following changes were requested to the paper: **To do: DZ**

- To identify that POL has not yet met expectations in Change.
- To identify how improvements to the way the Change programme is managed would be different to the previous attempts.
- To include a worked example where new governance procedures had worked.

7. Supplier Contracts out of Governance

7.1 The paper was taken as read.

7.2 The RCC noted that since the last meeting, there had been eight non-compliant incidents totalling £IRRELEVANT three of these being PCR (public contract regulations (2015)) breaches. One incident was of material value at IRRELEVANT. All incidents had failed to follow POL governance procedures with retrospective contracts required after the work had commenced. Overall, the non-compliance value had dropped slightly from IRRELEVANT in July to IRRELEVANT

7.3 The Committee discussed and sought to understand how work could be commenced without a contract or caf (contract approval form) being in place and requested that a "lessons learnt" report be produced. **Action: BB**

7.4 The Committee noted that discussions are in train with Marketing and IT on their upcoming renewals to identify appropriate sources required.

8. Policies for Approval

8.1 The policies were taken as read.

8.2 *Contract Execution Policy*
The Contract Execution Policy was **APPROVED** for submission to the ARC on 23 September 2019.

8.3 *Financial Crime Policy*
The Financial Crime Policy was **APPROVED** for submission to the ARC on 23 September 2019.

8.4 *Anti-Money Laundering and Counter Terrorist Financing Policy*

The Anti-Money Laundering and Counter Terrorist Financing Policy was **APPROVED** for submission to the ARC on 23 September 2019.

The supplementary HMRC Fit and Proper Standards Policy standard was also **APPROVED** for submission to the ARC on 23 September 2019.

8.5 *Physical Security Policy*
The Physical Security Policy was **APPROVED** for submission to the ARC on 23 September 2019.

8.6 *Modern Slavery Statement*

AC recognised the legal requirement to draft the statement but sought to understand the following points:

- How did POL ensure that modern slavery was not taking place within the agency network?
- The scale of extra resource required as suggested by the independent consultants Good Values (who reviewed POL's modern slavery statement and practices).
- The potential warning signs of modern slavery to be aware of.
- The internal on-boarding procedures of staff.

8.7 AJ and DS both remarked that it was difficult to assess whether slavery took place in the agency network, but explained that agencies were expected to complete due-diligence and background checks on all new employees. Additionally, employees are vetted before they join POL and Fit and Proper checks are completed on staff carrying out financial services activities.

8.8 In terms of additional resource required, AJ advised that this was a recommendation made by the independent consultants, but was not being requested at this point in time. The paper would be clarified for ARC.

8.9 Regarding signs to look out for, AJ suggested this included staff being provided with accommodation and signs of distress on sites visits. Raising awareness was key to avoid any modern slavery taking place within the agency network. The field teams had been advised of the signs to look out for, but to date no modern slavery reports had been made.

8.10 The Committee noted the difficulties in enforcing modern slavery and further noted that Payzone was not required to report (as it did not fit the required thresholds for reporting).

9. Deep Dive: FS Quality of Sales in the Network

9.1 The report as taken as read.

9.2 AJ commented that the quality of sales across the network was taken seriously and that MI data taken from the mystery shopping results had shown low instances of mis-selling, pressure sales, cancellations and complaints. However, it was noted the ability to follow the introductory sales process could be improved.

9.3 AK advised that the root cause had pointed to the need for better support to the client relationship managers in following the compliant sales process. He advised that following the introduction of three dedicated area managers to provide support and training on compliance to ensure CRM's are confident when dealing with customers, results had seen a marked improvement.

9.4 AC requested this be clearly stated in the paper for ARC.

10. Deep Dive: Monitoring of Multiple Retail Partners

10.1 The paper was taken as read.

POL00423464

10.2 KO advised that following engagement with BEIS, Risk, Finance and the Commercial Partnership teams, a tracker was established to monitor the financial stability of the five largest partners in terms of branches (these being...

10.3 The financial trackers mirrored those tracked by BEIS and are reviewed each period to show any outward signs of distress. These included:

- Profit warning
- Cash constrained – low liquidity headroom
- Prospective covenant breaches
- Poor financial ratios particularly gearing, operating margin, ROI/ROA
- Credit status downgrade
- Share price underperformance
- Failed refinancing
- New management team

10.4 KO explained that a financial RAG rating is prepared for each partner with the share price, trend, Experian ratings, key ratios and formal announcements all tracked. He reported that following a recent review, concerns had been raised with McColls performance, which was attributed to tough trading conditions. Wider contingency plans against partnership failings are in place.

10.5 The Chair requested this be continually monitored.

11. Deep Dive: Financial Controls

11.1 The paper was taken as read.

11.2 TL explained the financial reporting controls framework (FRCF) provided the first line of defence in the Financial Reporting Controls (FRC) environment. Since last review in 2017, the framework had grown from 241 controls (March 2017) to 500 controls (June 2019) with focus shifting towards enhancing the quality and ownership of controls. Feedback from the recent Internal Audit review was in line with expectations - that the underlying controls are appropriate, but that an advanced piece of software should be considered. It was noted that going forward, the breadth of the framework needed to be considered to identify whether other elements of finance should be captured, beyond Financial Reporting.

11.3 Two high risk gaps identified in the framework included the inappropriate or unauthorised user access in the new cash management system CWC, and the cash centre transactions not fully reflecte d within the finance software CFS. It was expected these risks would be rectified by December.

11.4 Accounting errors identified in 2017/2018 had highlighted the need to strengthen the second line of defence in the FRC environment. These included the balance sheet reconciliations and associated review processes, both of which have been redesigned.

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

The draft ARC agenda for 23 September 2019 was **NOTED** and discussed.

13. Any other Business

13.1 Meeting dates

It was noted that the next scheduled RCC meeting was on 7 November 2019.

POL00423464

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Belfast Datacentre Disaster Recovery Exercise

Author: Craig Bibby Sponsor: Shikha Hornsey Meeting date: 23rd September 2019

4

Executive Summary

Context

The Fujitsu operated Belfast Datacentre hosts Horizon our Post Office counter trading application, and other business critical applications. The resilience of this datacentre has not been completely tested since 2013 due to the high risk of recovery of some obsolete applications (POLSAP) and equipment in the legacy estate. Post Office policy for critical infrastructure is to conduct annual IT Disaster Recovery (DR) tests to ensure that should an incident occur we can be confident of these plans. It is also a commitment to a number of our partners, clients and our customers.

On 24th August 2019 a failover test was attempted, but could not complete. This paper provides an update on the test and recommends next steps.

Questions addressed in this report

1. How did the failover test go?
2. Has our risk position changed?
3. What are our recommended next steps?

Conclusion

1. There are lots of positives to take from the well planned test execution and many lessons learned. It's reassuring to know 6 years after the last attempt that the Horizon application and key live product integrations worked. However a number of small niggles delayed progress and ultimately at 2am an internal datacentre network routing issue was found. The rollback was successful and Post Masters were ready for trading by 5am.
2. Whilst we have higher confidence in our ability to failover, fundamental elements of a successful full DR test still haven't been completed and it can be argued that we haven't met our contractual obligations. Should the failure be made public, it could worsen our PR risk.
3. We explored 3 options: a full DR test over Christmas, a full DR test over May bank holiday, or a partial DR test October 12/13th followed by full DR in May 2020. Our recommendation is the final option as a partial test will allow us to confirm our trading platform works in a DR situation, materially changing our risk profile.

Input Sought

Agreement to proceed on Saturday October 12th to failover to the secondary datacentre, run a suite of model office transaction tests and failback before Branch trading operations on Sunday 13th.

POL00423464

The Report

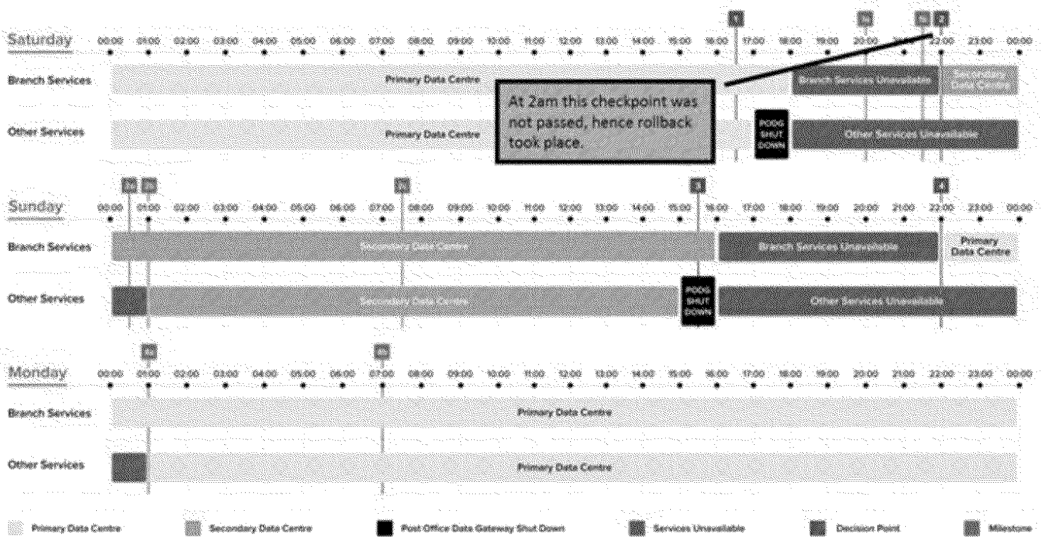
How did the failover test go?

All pre-test activities were completed successfully in the build up to the exercise, with one minor hardware issue reported and quickly resolved, culminating in a GO decision on Thursday 22nd August. Test environments were shut down and baseline testing performed on Friday 23rd August. The exercise commenced at 17:00 Saturday 25th August.

Time	Objective	Result
Saturday 17:00	Post Office Data Gateway (PODG) shutdown	Completed
Saturday 20:00	Controlled shutdown of the Primary datacentre and MasterCard disconnect Vocalink connection	Completed
Saturday 20:00 – 22:00	Failover to Secondary datacentre. Hardware and applications brought online.	Completed
Saturday 22:00	JPMorgan confirm Fujitsu online banking. Connectivity confirmed with DXC for POCA (Post Office Card Account)	Completed
Saturday 22:20	MasterCard implement Vocalink connection	Completed
Saturday 22:30	Connect Counters to the secondary datacentre for model office testing	Failed
Sunday 01:00	Restore PODG and Horizon online services in the secondary datacentre.	Not tested
Sunday 02:00	POL decision to regress and failback to primary datacentre	Completed
Sunday 02:12	MasterCard disconnect Vocalink connection	Completed
Sunday 02:15	Logs recovered, failback to primary datacentre initiated	Completed
Sunday 02:30	Failback to primary datacentre	Completed
Sunday 05:00	MasterCard implement Vocalink connection	Completed
Sunday 05:03	Branch trading restored	Completed
Sunday 06:00	Network banking connectivity confirmed	Completed
Sunday 08:00	PODG and Horizon online services restored, overnight batch initiated	Completed
Sunday 15:00	All back office file processing confirmed and validated	Completed

POL00423464

The plan below shows the checkpoint at which the test was halted. Horizon was available for trading the next morning by 5am, with all follow on batch files delivered to our clients and back office systems.



WHAT WENT WELL?

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

- Fujitsu's technical plan was robust with controls in place to regress, enabling POL to take the decision to protect service and assure no trading impact.
- Once a decision was made the failback procedure was executed quickly and branch trading ability was restored in good time.
- All hardware components and applications were stood up successfully in the secondary datacentre.
- The support of all key partners was very good, implementing changes to enable the test and providing support in diagnosis where required.
- The back office file processing was manually processed by Accenture with no customer impact, with POL users also validating data quality successfully.
- Proactive communications to branches were sent through all available channels, including customer information posters, posted to branches.
- Communication to our clients detailing the impact to trading and client files was largely effective, although 2 of 562 client's files were escalated by clients. These were quickly resolved during the exercise and have been added to our planning for next time.

WHAT WENT WRONG?

Technical and organisational improvements have been identified, with remediation plans detailed below.

POL00423464

Issue	Description / Resolution / Action	Status
Technical		
No Branch Access to Horizon	➢ The load balancer was hiding source IP meaning that the counter IP wasn't being sent through to the network reverse proxy for authentication. This was caused by incorrect source Network Address Translation (NAT) on the Citrix Load Balancers. ➢ There was insufficient time to resolve during the test but logs were taken. Fujitsu have now made changes, and technical teams have proposed how these can be tested prior to a full failover. ➢ Testing is planned for 28th September (more info included below in next steps).	Likely resolved, pending re-test
Counter policy routing	➢ Additionally, there was inaccurate policy based routing for counters and any traffic would not have been returned. This error was discovered after the test, on analysis of the network logs taken. ➢ Configuration change applied and issue resolved. ➢ Testing is planned for 28th September.	Likely resolved, pending re-test
Vocalink connectivity	➢ Vocalink connection was initially unsuccessful on failover, the issue was resolved and validated without any intervention. ➢ The route cause is being investigated with MasterCard. ➢ This does not impact the decision to retest.	Under investigation (does not prevent re-test)
Branch database storage	➢ Incorrect storage presentation to branch database, due to incorrect mapping. This caused a 30min delay during the August DR test, configuration was correct, storage represented and resolved during the test.	Resolved during August test
Communications		
Digital Channels	➢ Digital team did not have sufficient lead time to use all proactive customer channels. ➢ Communication team lesson learnt, this will be incorporated into communication plan.	Lesson Learnt
Client Engagement	➢ Two clients reported delayed files during the exercise, despite proactive communication of the exercise impact. ➢ This will be addressed with Post Office CRM's for Santander & Global Pay to ensure information is passed to client's Operational teams.	In Progress

POL00423464

Planning & Execution		
IT Service Desk	➢ The service desk did not inform callers directly that these issues were due to a planned test – although instructed too. ➢ This will be re-emphasised with the desk before the next test.	Improvement action for next time

Has our risk position changed?

BUSINESS CONTINUITY

Overall we perceive the risk to our business continuity has reduced due to the successful components and technical updates following lessons learned in the test. However some fundamental items remain untested.

Positive changes to risk position		Unchanged or negative changes to risk position	
Across the business and key partners the planned approach is well understood, and was working in practise.	↓	Branches could not connect to the Horizon application to perform any live transactions.	→
All applications were shut down successfully.	↓	A full day's volume of transactions did not occur.	→
The Horizon application was stood up in the secondary datacentre for the first time in 6 years.	↓	Failing back with additional transactions in the database (a slightly different process) was not completed	→
The live connections to banking (Vocalink), Paystation (Ingenico), AEI Booths (Thales) and payments were confirmed as active (although no transactions).	↓	Nightly batch integrations (PODG) were not processed from secondary datacentre, following a days transactions.	→

FACTORS IMPACTING OUR DECISION TO TEST

Prior to conducting the test we evaluated a number of factors. These are re-evaluated below.

Factor	Change in evaluation
Risk to trading in a disaster situation.	See section above - we evaluate that this risk has reduced. ➢ Known technical issues have been remediated with changes and a plan to test these fixes is in progress. ➢ Positively the applications were fully stood up in the secondary data centre with links to 3rd parties for live integration tested.

POL00423464

Factor	Change in evaluation
How long Post Office bears the above risk	This factor remains unchanged from when previously evaluated – it is still likely Post Office will remain on Horizon in the Belfast datacentre for some time, the Belfast Exit project has not re-started.
Commitment to clients & banking framework	Post Office policy commits to performing business continuity tests at least annually. It could be said that we've met the terms in the banking framework which states that Post Office should, "test and update their business continuity and disaster recovery plan annually. Post Office shall promptly implement any necessary remedial actions identified by or as a result of such tests", however it could also be argued that it is implied that the test should be successful.
Group Litigation Order and media coverage	Post Masters, clients and partners were communicated to frequently on the lead up to the test. It was also communicated that the second outage window was not required. Whilst we've not seen any media coverage on this issue, we can only assume that it could be known our DR test could not complete. A re-test will require further outages, but assuming it is successful we will at least be able to confirm our DR plans work adequately.
The risk of conducting the exercise	Having just completed a significant portion of the test, overcoming a number of issues on the way and safely failing back. This risk is somewhat reduced.

What are our recommended next steps?

We have seriously considered 3 options. The first two follow the same process we followed for this bank holiday; failover on a Saturday, full day's trading on secondary on Sunday, failback to primary for bank holiday Monday. We haven't considered a non-bank holiday weekend due to the increased risk to trading. Our options are:

1. Full test May 2020 bank holiday
2. Full test over Christmas
3. Partial DR test on October 12th followed by full test in May 2020

In all cases we first need to confirm that the network issues that prevented success in August have been resolved. This in itself requires some Branch downtime.

ISOLATED NETWORK TEST

The proposed way to test the network without full application failover is to route all live counter transactions through the secondary network, whilst all applications remain uninterrupted in primary. Switching the network requires at best a 3 minute downtime for the network. We've selected 10pm on Saturday when we expect c.505 branches to be open, with between 1-4 transactions a minute across the network. We will communicate the following to Post Masters:

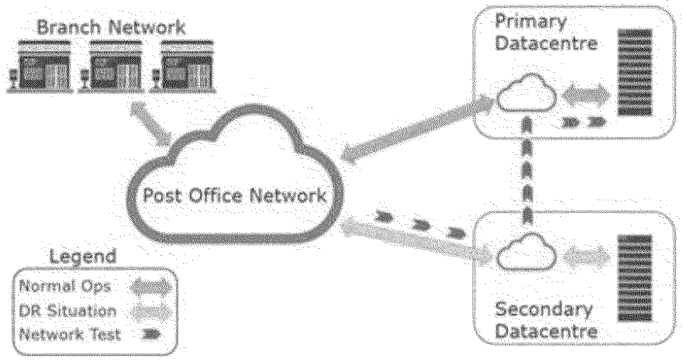
POL00423464

10pm – 10 min downtime. Error message displayed in Horizon

10:10 – Normal trading resumes. Model office testing begins

10:40 - 10 min downtime. Error message displayed in Horizon

10:50 – Normal trading resumes



DR TEST OPTIONS

1. **Conduct a similar test over May 2020 bank holiday**

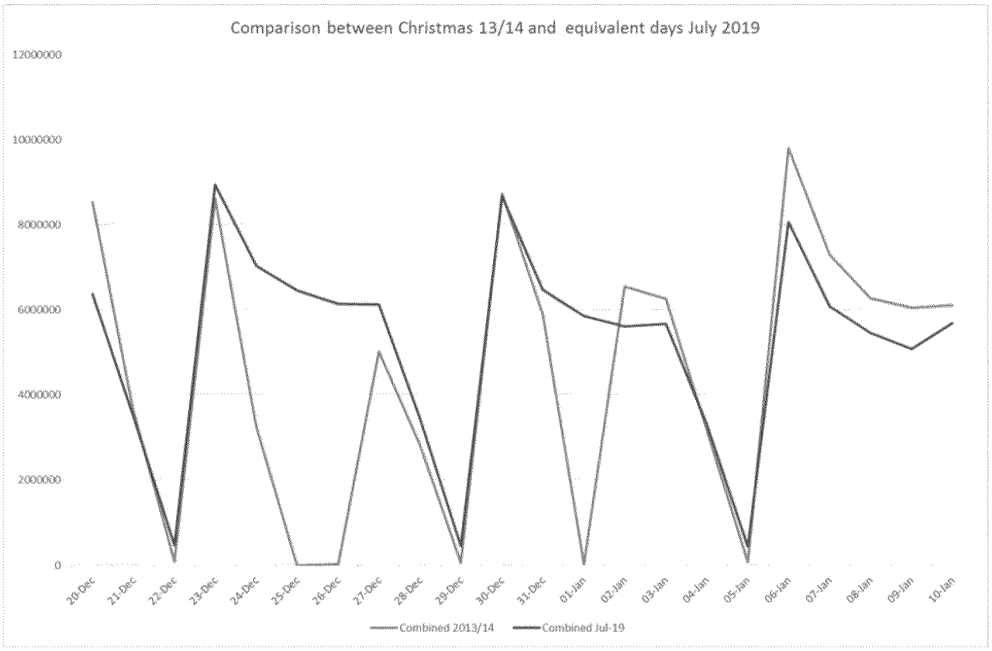
The plan and approach for this is clear, however it means retaining our current risk until May 2020.

2. **Conduct a similar test over Christmas**

Perform a full test during the Christmas period. The graph below shows transactions for the last Christmas that fell on a Wednesday, compared to an average week. The opportunities to run a day's test on secondary with lower transactions than usual are the 24th, or 31st meaning failover would start on the 23rd, or 30th.

This is technically possible but we judge the potential PR risk to be higher due to the time of year. Additionally whilst we have time to lock-in resources, some important people within Post Office and are partners will no doubt be unreachable.

POL00423464



3. **Partial DR test on October 12th, followed by full test in May 2020**

Over a standard weekend we do not want to fail to secondary for an entire day due to the increased risk to trading on the Sunday or Monday due to issues in failback. However we have technically planned for a fail over – fail back in one evening.

The proposal is to:

- Saturday 28th Sept - Confirm the network issues have been resolved by routing network traffic temporarily through the secondary data centre (pre-requisite to the below).
- Saturday 12th October 6pm – Failover to secondary datacentre. Conduct transaction and live service testing from Model Office 10-2am. Failback to primary confirming all transactions are correctly reconciled.
- Sunday 13th October 6am – Primary System available for trading.

This would materially improve our risk position (see updated table below) having confirmed our trading platform can failover as planned. We are investigating also bringing up PODG in our secondary datacentre and using a test file to demonstrate that batch processing could occur. This would turn the bottom right arrow partially green also.

POL00423464

Positive changes to risk position		Unchanged or negative changes to risk position	
Across the business and key partners the planned approach is well understood, and was working in practise.		Connection from branches to Horizon for live transactions would have been confirmed	
All applications were shut down successfully.		A full day's volume of transactions did not occur.	
The Horizon application was stood up in the secondary datacentre for the first time in 6 years.		Failback to primary with transactions conducted in secondary would have been tested.	
The live connections to banking (Vocalink), Paystation (Ingenico), AEI Booths (Thales) and payments were confirmed as active (although no transactions).		Nightly batch integrations (PODG) were not processed from secondary datacentre, following a days transactions.	

Following this we would wait until May 2020 to complete full annual DR, and maintain the schedule annually going forwards.

POL00423464

POST OFFICE

AUDIT AND RISK COMMITTEE

PCI Compliance Status Update.

Author: Phey Rasulian Sponsor: Shikha Hornsey

Date: 23rd September 2019

5.1

Executive Summary

Context

The PCI Programme issued an update to RCC on the 3rd September 2019, this paper provides a progress update across the programme covering all significant activities across the three workstreams: IT, Target Operating Model (TOM) and Branch/Client Communications (Comms).

Questions this paper addresses

1. What progress has the IT workstream made, providing Point-to-Point Encryption (P2PE) & Banking Transaction Processing Solution?
2. What progress has been made exploring the feasibility of the fallback solution?
3. What progress has been made to change the Post Office's operating model to ensure process/products comply with PCI?
4. What communications have been issued to the Post Office's client base and what if any feedback has been received?
5. What is the overall timeline for achieving full PCI compliance, across all workstreams?

Conclusion

1. VocaLink, Fujitsu and Ingenico have been continuing detailed design activities with the aim to capture all technical requirements of the proposed solution. All activities are progressing as planned.
2. In parallel with progressing the detailed design, Post Office are exploring two other routes to provide an outsourced capability to process both retail and banking transactions in a PCI compliant manner. A feasibility study is underway to explore if either of the alternative options can provide the capability faster and at a lesser cost.
3. Problem analysis of all suspected non-compliant products and processes has concluded, and the next step will be to commence the solution analysis.
4. The Programme continues to regularly update our clients, acquirers and Qualified Security Assessor as to our plans for regaining compliance. The latest set of communications was issued this month and no negative feedback has been received.
5. Ingenico have provided an indicative high-level plan that denotes rollout concluding in February 2021. The programme has communicated that delivery needs to completed as early as possible within 2020 and not to extend into 2021.

POL00423464

Current status

1 Point-to-Point Encryption (P2PE) & Banking Transaction Processing Solution

1.1 *Pin pad rollout* - The rollout of P2PE enabled pin pads is underway with the agreed plan for collection, shipment, and firmware upgrade and in-branch device swap-out. Deployment into the model office and first week of a three week pilot has been completed. Four minor issues were encountered and have been rectified. Depending on the pilot concluding successfully, full swap out ramp up to 1000 pin pad per week will commence on 23rd September.

1.2 *Banking transaction processing solution* - Detail design activities and workshops continue to be completed as per the design phase schedule provided by Ingenico, remaining on target to complete by October 2019.
There is ongoing dialogue with our Qualified Security Assessor (QSA) from Nettitude and the Post Office's main acquirer Global Payments to ensure they are aware and remain supportive of our approach.

1.3 *Commercials* – The Programme has requested a plan from Fujitsu which should include a timeline for the deliverables and commercial activities that are required to ensure all costs can be collated at the earliest possible opportunity. Ingenico have stated that they will release further details on the cost and timelines post detail design completion in October 2019. The Programme has asked Fujitsu to push to achieve cost and timeline visibility sooner.
Ingenico asked for an indemnity against any regulations other than PCI DSS that they may need to be compliant with. The Post Office legal team discussed the matter with Ingenico and impressed upon them that there were no regulation other the PCI-DSS that they needed to be compliant with. Ingenico sought their own legal advice and drew the same conclusion. Ingenico have stated that there are still specific conditions that they wish to include in the contract. The Post Office legal team will explore this further once the exact wording has been released.

1.4 *Fallback Alternative Solutions* – Workshops and a feasibility comparison has taken place between the FIS Global offering and the indicative costs and timelines received from Ingenico. Currently, there has been no significant indication that FIS Global will be able to deliver the solution quicker or more cost effectively. However, FIS Global's operating costs are significantly lower than the initial pricing Ingenico have provided. A similar activity is being conducted with ACI Worldwide.

2 **The PCI programme Target Operating Model (TOM)**
The TOM workstream is looking activities that resulted in PCI non-compliance and improving the vetting of those activities. These will include,but are not limited to, training, change process changes to incorporate PCI compliance checkpoints and card data scans.
The product and process initial remediation has been published and is forecasted to complete solution analysis by Q1 2020. This will be conducted in an iterative manner

POL00423464

enabling the programme to incrementally remediate products and processes as they are ready to be released.

3 **Communications to the Post Office's Clients and Branches –** Communications summarising the progress the Post Office has made towards regaining PCI compliance has been issued this month to all banking clients and 50% of the non-banking clients. A three slide update pack has been generated that will be updated monthly and issued to those clients that have requested amonthly update. Branch communications have also been compiled, reviewed and approved ready to be issued to the network once the pin pad pilot has completed successfully.

4 **Timeline to regain PCI Compliance –** The overall timeline for completion that is, receiving a Report of Compliance, is forecast between Q4 2020 and Q1 2021 due to Ingenico's timelines. The deployment of pin pad refresh element of P2PE solution has a high level of certainty and has already started to rollout as mentioned above. The other areas are steadily improving their levels of certainty as the Programme progresses through its lifecycle. The next significant milestone will be October 2019 when the firm costs and timelines will be released by all third parties. All avenues are being explored to shorten the timelines. All third parties are aware that this is one of the Post Office's highest priorities and it has continued to be impressed upon the third parties that the delivery timeframe needs to be shortened at every opportunity and deliver no later than December 2020.

POL00423464

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Cyber Security Update

Author: Tony Jowett/Jenny Ellwood Sponsor: Shikha Hornsey Meeting date: 3rd September 2019

5.2

Executive Summary

Context

This paper describes how we are increasing the maturity of our cyber defences, what are the early results of two initiatives delivered as part of this and how we have assurance that there are no effects of the Capital One breach on Post Office.

Questions this paper addresses

- What progress have we made in achieving our maturity targets?
- What results are we seeing from our threat intelligence partners Recorded Futures?
- What results are we seeing from our Security Operations Centre?
- What is our proposed cyber risk appetite?
- What additional data do we have regarding the Capital One incident?

Conclusion

1. We have completed all key recommendations from the Deloitte review. We continue to deliver on the highest priority actions on the detailed recommendations. Detailed progress is included in this paper and a plan is included in the Appendix. We continue to be on track to reach our target maturity by March 2020 whilst recognising that in subsequent years we will need to continue to deliver security improvements in response to changing business needs and threats.
2. Our threat intelligence provider has given us advanced warning of threats to the post office that we otherwise would not be aware of. Threat intelligence information is also being shared with other areas of Post Office such as operations and financial fraud.
3. The SOC also has been instrumental in responding to the large number of incidents across the estate which would be invisible otherwise. We continue to expand the coverage of the SOC on a risk and cost ranked basis.
4. We propose to adopt two risk appetite levels: “Averse” and “Neutral” depending on the nature of the data involved.
5. There have been no known major internal incidents. Following up from previous external incidents we have met with the CISO of Capital One to further clarify if there is any potential impact on Post Office

Input Sought

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

POL00423464

Report

What progress have we made in achieving our maturity targets?

1. The **Key Recommendations** from the Deloitte Review are shown in Appendix A. We have now completed all of these with sign off from Internal Audit.

2. Our target maturity levels were explained in the previous report. We have included a Gantt chart showing the plan for the IT Security Transformation Programme (ITSTP) Appendix B. We are aiming to hit target maturity by March 2020. In subsequent years we will need a rolling programme of security improvements to keep Post Office safe in response to developments in the business, the changing nature of the threats faced and the opportunities arising from developments in defensive technology.

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

Area	Milestone Completion			Target Completion Date	Update
	Target	Previous	Current		
Deloitte Cyber Review Actions	45%	48%	52%	March 2020	Continue as planned. Key areas where improvements have been made include incident and crisis management, patch and vulnerability management and processes around secure software development.
Deloitte Information Protection Review actions	40%	30%	45%	March 2020	Continue as planned
RSA Archer implementation	30%	3%	31%	Feb 2020	Delayed start, now in catch up mode due to organisational blueprint delivery date. Plans developed and delivery commencing early Sept19
DLP	10%	0%	13%	Feb 2020	Discovery phase commenced with initial CRs for data capture being delivered WC 19th Aug – Phase 2 planning dependant on discovery analysis and results.
SOC Maturity	Treated as ongoing continual improvement to BAU. Widening coverage of SOC through acquisition of more logs including Payzone and Post Office Insurance.				

POL00423464

4. Based on this assessment the gap between the current and target maturity levels of Post Office has been reduced by 44% (last report was 23%) since the start of the programme in March 2019.

5. We have commenced regular Security reviews with our major suppliers to assure they are governing themselves in line with our Cyber Security policy and Standards through our existing governance fora. In addition, we are implementing the RSA Archer Third-Party Risk modules to improve the overall visibility of our Third-Party vendor risks. The questionnaires that were completed initially in OneTrust by the suppliers and the manual reporting that has been used to date will be ported into RSA Archer to ensure one source of the truth for the Third-Party (and their own suppliers') security risks.

6. We have also recently implemented Recorded Futures as our Threat Intelligence partner which provides additional Third-Party Risk scores that can be used within RSA Archer.

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

What results are we seeing from our threat intelligence partners Recorded Futures?

8. To stay focused on current risks we have taken onboard a Cyber Threat Intelligence supplier – Recorded Futures (RF) to replace Digital Shadows. The RF tool scans the web searching for any mention of Post Office interests and automatically alerts Post Office security to potentially harmful threats.

9. RF data is being sent to other departments in Post Office including Fraud, Risk, and Data Protection. This establishes greater oversight of the cyber threats that are 'out there' and helps to protect the brand.

10. The table below summarises what we have done to date.

What we've done	Why we've done it	How it protects us	Outcome
Established the Recorded Future tool across the business. (Fraud, Brands, etc . . .)	To help POL see the 'bigger picture' with regards to the Cyber threat landscape	POL now gets intelligence fed directly to it's different departments enabling better protection all around.	Advanced warning of threats allowing early action to be taken
Implementation of Threat Intelligence Platform (TIP)	A TIP allows POL to receive various threat intelligence feeds into one single platform thereby obtaining an holistic oversight into threats	Provides additional understanding and background to help when investigating the incident. This allows the business to intelligence into strategic decisions	A single pane of glass that shows where POL are potentially vulnerable
Established a working group between Brands, Legal and Security	To mitigate potential fraud and risk to the brand	Allows us to prioritise and remediate fraudulent websites that potentially target vulnerable customers	A joined-up approach to assess the risk to Brand and mitigate it

11. We have had over 30 alerts from RF since start of service which we would have been blind to without RF. Three notable examples are:

POL00423464

a.

b.

IRRELEVANT

c.

d.

What results are we seeing from our Security Operations Centre?

12. A Security Operations Centre (SOC) is the hub of all security operations. Current cyber-attacks aim to be as quiet as possible for as long as possible to avoid detection. The indicators that an attack is taking place are subtle. The SOC's main job is to join disparate information in real time to determine what is and is not a real attack. The SOC also acts as a coordination point for rapid and accurate incident response and recovery from an attack. It also is a source of data for development of cyber defences.

13. In Post Office we have the following SOC arrangement

    a. An in-house SOC team staffed during normal working hours (with on call arrangements) covering second and third line responses. All incident management and response is coordinated through this team.

    b. An advanced SOC (ASOC) first line team running 24x7 within Verizon's Managed SOC in Dortmund.

    c. Event log feeds from systems and infrastructure run on our behalf by Accenture, Fujitsu and Computacenter to the Verizon ASOC.

    This approach balances the contribution from our third parties with the need to retain in-house capabilities so that responses can be coordinated across the business and third parties.

14. The SOC was established and went into learning mode in November 2018 and was operational in April 2019. From April – July 2019 a total of 792 tickets were handled by the Verizon ASOC with 77 tickets being escalated to the Post Office SOC team. Examples of the escalated tickets are:

a.

b.

IRRELEVANT

POL00423464

c.

d.

IRRELEVANT

15. We are continuing to mature SOC processes and policies. We are extending SOC coverage on a risk and cost-weighted basis across the estate.

What is our proposed Cyber Risk Appetite?

16. A review of the existing 2015 Data Risk Appetite Statement has been carried out and a recommendation is made to introduce a new Cyber Risk/Data Security statement.

17. Whilst the 2015 statements were broadly accurate, the statements were high level, difficult for the business to interpret in their decision-making process and to monitor whether they remain 'within' or 'outside' of risk appetite. It also did not recognise that not all data needs to be managed with an 'averse' appetite.

18. The original 2015 Appetite statement is shown below:

Principle Risk	Appetite
Technology Systems and IT related risk; stability, design, implementation. This also includes IT Security, hacking, and unauthorised use of data.	Averse risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences

19. The new revised risk appetite statements are as follows:

POL00423464

Principle Risk	Appetite
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.	**Strictly Confidential / Confidential Data or Data that has a High CIA score** **Averse** risk appetite for the loss of the above data categories which could lead to financial loss, business disruption, public embarrassment or legal consequences. (Example: Data within this category would likely be, but no be limited to personal/sensitive data or be business critical by means of content). **Internal/Public Data or Data that has a Medium to Low CIA score** **Neutral** risk appetite for the loss of the above data categories which could lead to financial loss, business disruption, public embarrassment or legal consequences. (Example: Data within this category would likely be binary by nature, contain no personal/sensitive data and not likely to affect business strategy).

20. The harm table used to assess the impact and probability score has been reviewed (Appendix C) and enables the business to understand what the term 'averse' translates into. Essentially, we recommend for an 'averse' appetite that we maintain a 'Green' risk target score for the compromise or loss of personal/sensitive data. For data which does not contain Personal / Sensitive or Business Critical Information we adopt a 'neutral' appetite.

21. A scorecard has been developed to track how Post Office is performing against Risk Appetite for Cyber and Data Security (shown in Appendix D). This is reviewed alongside any risks 'outside' or close to being 'outside' appetite by the Information Security Committee.

What data do we have regarding the Capital One incident?

22. Post Office signed a deal with CapitalOne on 28 June 2019 to provide credit cards to Post Office customers. As a new deal we have yet to sign up any customers, but we are targeting a customer base in excess of 500,000.

23. Capital One experienced a IRRELEVANT IRRELEVANT We understood that there was no impact on the Post Office, but we met with Capital One's CISO Neil Barlow on the 14th August 2019 to further clarify the nature of the hack and be reassured that this was the case.

24. Neil explained that

a. IRRELEVANT

b.

c.

25. Capital One US are now implementing the necessary controls to avoid a repeat occurrence and Capital One UK have reviewed their controls and are confident they would not experience the same IRRELEVANT Based on this discussion and our own investigation the controls in place in Capital One UK would adequately protect Post Office IRRELEVANT

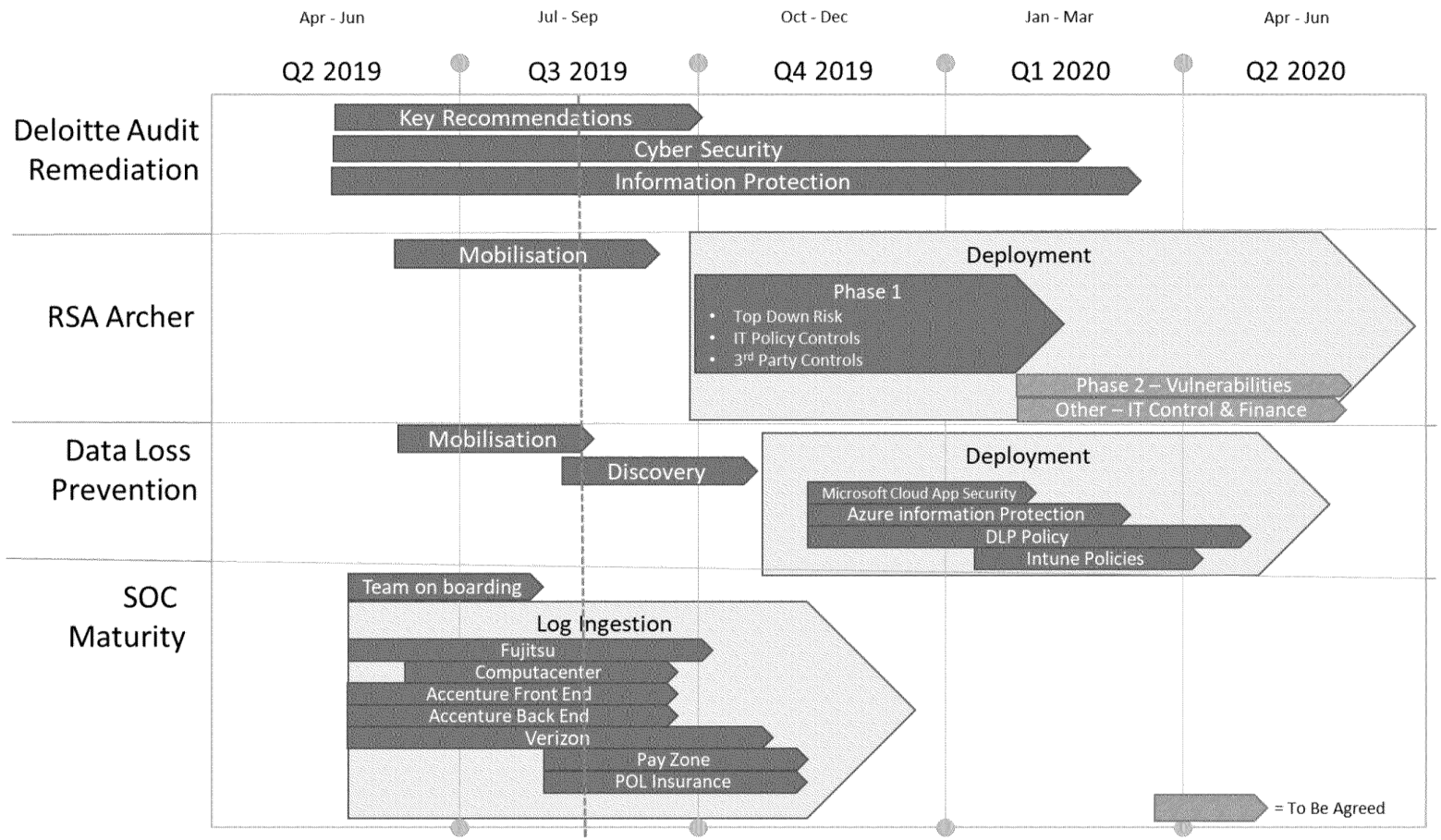
POL00423464

Appendix A Deloitte Key Recommendations

1. Confirm Principal IT risks and risk appetite statements (specifically including the Cyber Security risk)
2. Create a prioritised list of crown jewels.
3. Agree target maturity levels for all Cyber Security domains.
4. Perform a gap analysis between the IT Security Transformation Programme (ITSTP) and the recommendations from this review
5. Update the ITSTP to address any gaps from the gap analysis.
6. Implement a mechanism to track and report progress against the ITSTP
7. Review, finalise and share cyber risk metrics with a view to regularly reporting a dashboard to the Board.
8. Develop Post Office's Cyber Threat Intelligence (CTI) capability in order to proactively inform decision making across the business by agreeing a framework for CTI.
9. Develop Post Office's Resilient capability by fully documenting BCM procedures and processes in respect of cyber resilience
10. Develop and agree an Insider Threat Programme

POL00423464

Appendix B ITSTP 2019/20 Plan



POL00423464

Appendix C - Harm Table and Supporting Heat-Map

RISK SCORING	IMPACT ON: Financial (inc. strategic)	Operational (inc. people, change technology, information security)	Customer	Reputational (inc. third party, legal and regularity)
Critical - 5	**£20m>** or could have a long term impact on commercial viability	– Exceeds operational capacity to respond, breach of Government commitments – Fatality and/or prosecution – Loss of critical system or complete network outage	– Significant boycott of products and services – Breach of coverage or scope of services to meet social purpose or entrustment	– High profile legal case – Maximum regulatory penalties, removal of ability to operate, public enquiry – Complete loss of confidence e.g. staff, clients, partners, customers – Sustained hostile national media coverage and online narrative
Major - 4	**£5m> - <£20m** or could substantially weaken the business	– Major operational impact felt throughout the business – Multiple major injuries – Partial loss of critical systems or critical IT vulnerabilities left unpatched	– Alienate/lose a significant group of customers, Postmasters or partners	– Material legal dispute with negative outcome – Substantial censure sanctions imposed or large scale penalties, material customer detriment – Minister exercising powers, parliamentary inquiry – Major adverse national media campaign
Significant - 3	**£100k> - <£5m** or significant effect on achieving business objectives	– Operational impact felt in multiple areas – Major injury with adverse HSE outcome or multiple minor injuries e.g. assault on branch – Significant loss of systems	– Customer / Postmaster dissatisfaction impacting business achieving objectives e.g. innovation – Safeguards and controls to protect vulnerable customers	– Reportable to regulators, minor sanctions, small fines, minor/no customer detriment – Minister discussion – Substantial adverse national media campaign
Moderate - 2	**£50k > - <£100k** or moderate effect on achieving business objectives	– Small operational impact felt to a single area – Minor injury with adverse HSE outcome or major injury with no personal liability outcome – Moderate loss of non critical systems	– Small number of customers contained within 1 product or channel, or where there is no scope for customer, Postmaster or partner detriment	– Low level repeated penalty breaches e.g. waste water – Adverse notification from regulators – Some adverse media and online reaction
Minor - 1	**£0> - <£50k** or negligible effect on achieving business objectives	– No measurable operational impact to business – Minor personal injury with accidental outcome – Insignificant loss of systems	– No or very minor customer impact to a small number of customers, Postmasters or partners	– Low level legal issue – No regulatory impact e.g. penalty notice – Little media / online reaction

	Remote - 1	Unlikely - 2	Possible - 3	Likely - 4	Almost Certain - 5
Critical - 5	A	A	A	A	A
Major - 4	N	N	A	A	A
Significant - 3	T	N	N	A	A
Moderate - 2	T	T	N	N	N
Minor - 1	T	T	T	T	N
	Almost an inconceivable event	Event is unlikely but could occur	Event is still unlikely but more possible to happen	Risk will probably occur in most circumstances	Risk is expected to occur in most circumstances or has materialised
	LIKELIHOOD				

Averse Appetite - High CIA Score within Cyber/Data Security Remediation/Control required to reduce the risk

Neutral Appetite – Low/Medium CIA Score within Cyber/Data Security Remediation/Control may not be required if the data does not contain personal/Sensitive Information

A = Averse
N = Neutral
T = Tolerant

POL00423464

Appendix D - IT Security KRI Examples – July 2019

KRI	Trend	KRI Status	Activity	Coverage
SOC Security Alerts	⟷		16 tickets in June escalated to Post Office Analysts to investigate further. 39 resolved tickets in June. Now monitoring O365.	43%
Firewall Assurance	↑		All feeds are now in place and working – Remediation work to continue until completion	85%
Anti-Virus	⟷		Status switched to green. SEP14 progressed to phase 2 and operating effectively.	95%
Email Protection	⟷		Mimecast provides the first level of defence against malicious email, 57.95% of inbound email was blocked this month which is lower than May but above the 12 month average (55.8%).	100%
WAF – Website Protection	⟷		No DDoS attacks detected in June.	100%
Threat Protection	↑		Service Now and Fujitsu both alerted in Recorded Future threat intelligence tool. Alerts remediated and stored on POL threat intelligence library for future reference.	100%

Note: All ***'Red/High Amber'*** Cyber/Data Security Risks will be reviewed within the Monthly Information Security Committee (ISC) Meeting, chaired by CISO.

RAG	Risk
	High Risk - Urgent Attention required and operating outside of target/coverage
	Medium Risk - Operating effectively but has not yet reached agreed target/coverage
	Low Risk – Operating within target and coverage

POL00423464

POST OFFICE

AUDIT AND RISK COMMITTEE INFORMATION ONLY

Transformation Office Changes

Author: Dan Zinner Sponsor: Al Cameron Meeting date: ARC 23 September 2019

Executive Summary

Context

The Interim CEO recognised that improvements to the Change process were not happening quickly or rigorously enough, separated the change accountability from the COO and hired a CTO (Chief Transformation Officer), reporting to the CEO, to provide much greater challenge based on a more precise understanding of individual projects. Before the CTO was hired, the COO centralised the Change functions with 9 portfolios of change and one large "Without Portfolio" portfolio. All 9 portfolios had an appointed Portfolio Lead and Business Sponsor, who both collectively were responsible for the strategy, direction and timely delivery of their Change portfolio. The stated objective was to "bring the systems of management and delivery closer together to improve visibility and control, simplify governance, speed up decision making, minimise silo'd working and reduce costs." Details of the initial centralisation efforts and Change Excellence programme can be found in **Appendix A**. In addition to the governance frameworks and line management changes, a separate team, the Change Risk & Assurance (CRA) team (which sits within the Central Enterprise Risk function), worked along-side the SPO to provide separate outputs. This was separate to Internal Audit's own separate, complementary audits.

6

In July, the ARC Chair requested an update from the new CTO. The CTO observed organisational confusion regarding the changes and a lack of consistency in the implementation of stated objectives. As POL had not yet met expectations for Change capabilities/maturity, and the embedding of the new Change Excellence programme was still in process, it was clear that an augmentation and acceleration of the approach was needed. Nonetheless, Internal Audit anecdotally noted positive control improvements and 3 areas of improvement: role clarity, 'best practice' examples and further organisational alignment to the new Change ways of working.

Questions addressed in this report

1. What is the current short term focus of the CTO and what changes are proposed?
2. What longer term changes are suggested and what are the triggers for these changes to occur?

Conclusion

1. The CTO's focus for the short term is to build on the COO's centralisation and create consistency in approach by: 1) identifying capable and competent resources to be placed on appropriately configured on teams; 2) increasing organisational clarity and

POL00423464

accountability; 3) raising the quality of support and challenge earlier in the process; 4) increasing the frequency of portfolio oversight with new routines, rhythms and reports to speed up issue identification; 5) broadening stakeholder understanding of, and conviction for, how 'Change works' at the Post Office to make the process more efficient, and; 6) assisting with GE to role model and embed a consistent way of working to improve the quality of planning and control. Explicitly the CTO plans to focus on improving the oversight and delivery of change ('doing things right') not on strategy ('doing the right things'). The plan has 3 areas:

People:

a. Structure Change teams that are fit for purpose and leverage current resources to ensure people are working within their scope and ability
b. Increase the number of capable and affordable Change resources, not necessarily total resources
c. Clearly communicate value of the centralised Change support team structure and roles and constantly ensure this is fit for purpose and cost

Process:

a. Operationalise Change routines and rhythms, ensuring consistency and speed across the business
b. Embed the Governance process and tools, with improved efficiency, effectiveness and agility
c. Actively manage the overall Change Portfolio by raising and resolving issues, making decisions, creating transparency and prioritising change activities

Perception:

a. Foster understanding, conviction and alignment within the Change community on how the PO "does Change," which includes training and constant "on the job" practice in new ways of working
b. Bring management along on the overall change vision and journey
c. Communicate the wider Change story across all areas of the Post Office

2. The key to success is creating transparancy and consistency across the organisation while intervening earlier in the process to mitigate downstream issues. This is a change in approach from earlier desire to create "Agile" project delivery and will require appropriately skilled, central SPO resources (recruitment in process). Once the organisation demonstrates and role models consistently it's ability to handle complex changes at pace, there is the possibility to review Change at the Post Office, similar to best practice organisations: Change "organisation as an organism," with cross-functional Agile teams, multiple 'speed of change' delivery models, etc.

Input Received

Portions of content provided in this paper have been shared with various members of the Group Exec, the Risk Director, the Finance Director for Change and the CTO's

POL00423464

direct reports. Feedback was directly sought from the CEO's of Retail & FS&T, and some of the questions to address in this paper are a result of this feedback.

Input Sought

This update is for approval by the RCC on the direction of travel of the changes laid out in this paper, which specifically address the delivery of Change at the Post Office.

The Report

1. What is the current short term focus of the CTO and what changes are proposed?

1. The CTO's short term plan is to embed Change processes and ways of working through consistency, clarification and communication. The plan emphasises the immediate need to focus on the Change community first by increasing understanding on how to consistently manage and resource a project for delivery (and thus implicitly not focus on "strategy"). This seeks to embed the former COO's original changes (centralised Change organisation and Change Excellence), while raising the quality of management and challenge and simplifying changes to further engage the overall business on Change. The plan includes a focus on People, Process and Perception.

2. The first immediate area of focus is about **people**. Specifically:
    1. Structuring Change teams to be fit for purpose. This means:
        - Leveraging available resources to work within their scope and ability (e.g., not appointing SMEs as Project Managers because "they know the content.")
        - Identifying appropriate roles, structure and number of resources required to deliver a project on time, to approved benefits. This may include having more resources, higher cost resources or clearly identifying the role of a resource (e.g., Product Owners appointed from within the business).
        - Challenging current team structures or requested resources for teams, earlier in the process. This is enabled by centralising all project resource requests, allowing for visibility on new team needs.
    2. Increasing the number of capable and affordable Change resources, not necessarily total resources. This means:
        - Leveraging the current Spans & Layers project to review Change resources and job families to be fit for purpose.
        - Through centralised and constant recruitment, creating a pipeline of skilled Change resources evaluated against clear competency frameworks in skills pools, balancing permanent, fixed term and contractor resources.
        - Actively managing and developing a pool of skilled internal resources (PMs, PMOs, BAs) to the quality required across the business, and not immediately

POL00423464

building further capabilities (e.g., Agile, People Change, Internal Consulting) until we demonstrate the value of current internal skill pools.

3. Clearly communicate value to the business of the centralised Change support team structure and roles (Central SPO, Portfolio Leads, etc.) and constantly ensure this is fit for purpose and cost. This means:
   - Engaging multiple stakeholders on the purpose and responsibilities of a centralised Transformation team (see **Appendix B1**). The creation of additional lines of defence, specifically Portfolio Leads (line 1b) (see **Appendix B3**) and a centralised, cross-functional SPO (line 2) (see **Appendix B4**).
   - Reducing the total number of Portfolios and ensuring all Change activity is included in a portfolio to have closer scrutiny and management of Change. (see **Appendix B2**).
   - Defining the roles and responsibilities of a centralised Transformation team (see **Appendix B3-B4**).

3. The second immediate area of focus is about **process**. Specifically:
   1. Operationalise Change routines and rhythms to ensure consistency, transparency and speed across the business. This means:
      - Embedding change by improving the consistency of management and reporting, through a new "Change Heartbeat", creating a new set of routines and rhythms to focus on the key Change areas: financials, risk, status, timelines, resources, dependencies/constraints. (see **Appendix B5**)
      - Centralised Change management information and reporting to all reporting on Change is consistent, accurate and from one source. This function will streamline and speed up reporting using an accurate, centralised database.
      - Creating a consistent set of dashboards, weekly reports and Steering Committee pack formats for Portfolio Leads so that the business and project Sponsors are constantly keep engaged and updated on portfolio and project progress to mitigate risks and issues in a timely fashion.
   2. Embed the Governance process and tools, with improved efficiency, effectiveness and agility. This means:
      - Educating the change community on ServiceNow (centralised Change database), spot checking and improving Change data, identifying ways to increase the useability of ServiceNow.
      - Running an 'embedding and continuous improvement' programme for Change Excellence Framework, within, not separated from, the Governance function. The continuous improvement programme focuses on usability of current principles, artefacts (e.g., best practice documents) and processes rather than creating new frameworks.
      - Engaging earlier and more frequently on prove/business cases from additional stakeholders before they arrive at approval Forums, including the CTO, PLs and SPO team members (e.g., RPOS business case delays to ensure clear articulation of the opportunity and benefits).

POL00423464

- Improving the quality of discussion and challenge at approval Forums through deeper questioning of projects (focused on delivery questions of "doing things right" versus strategic "should we do this" questions which are assumed to be answered ahead of time), closer scrutiny of material provided, sending questions to project in advance for presentation, giving more time for discussion at approval Forums by reducing the number of "big" discussions each week through planning ahead (e.g., multiple challenges to Digital Mails business case through multiple Forums).

3. Actively manage the overall Change Portfolio by raising and resolving issues, making decisions, creating transparency and activity prioritising change activities. This means:
   - Constantly reviewing cross-portfolio themes (e.g., interdependencies, constraints, risks, resources, finances) at a joint SPO and PL monthly meetings (taking place 2-3 times a month).
   - Bringing together multiple resources in one cross-functional SPO organisation, including dotted line management of risk, comms, finance and IT (note exact IT involvement is still a work in progress with the new CIO).
   - A more frequent focus on Change finances, including creating monthly (rather than quarterly) forecasts with finance business partners and better financial visibility (e.g., full transparancy on HIH costs through allocation of costs to various products that request HIH work).

4. The third immediate are of focus is about changing **perception**. Specifically:
   1. Foster understanding, conviction and alignment within the Change community on how the PO "does Change." This means:
      - Training and constant "on the job" practice in new ways of working for our Change resources, though Portfolio Lead mentorship and informal SPO training on new ways of working (e.g., weekly "drop in surgeries", email help line, face to face training).
      - Communicating more frequently, and quickly, to the total Change community on Change updates (e.g., Q&A sessions every 3 weeks).
   2. Bring management along on the overall change vision & journey: This means:
      - The CTO to use weekly GE updates, change reporting, Business Sponsors meetings and other management forums to provide constant Change updates using new reports from ServiceNow (still being developed).
      - Requesting the GE to role model appropriate behaviours of change management, including decisiveness and consequence management while advocating consistency, transparency and following governance rules and ensuring the best, right resources are on change programmes.
   3. Communicate the wider Change story across all areas of the Post Office. This means:
      - Engaging the Group comms teams into the overall Transformation story allowing for a coherent and constant feed of change communications through multiple existing comms channels, for various stakeholders

POL00423464

2. What longer term changes are suggested and what are the triggers for these changes to occur?

5. Given the lower level of change maturity at the Post Office, in the short term, there is a need to centralise all Change under one clear approach to raise overall capabilities for change. This may be a short to medium term need (up to 24 months) while the business learns and demonstrates Change maturity. The main purposes of creating one centralised team and approach are: 1) clearer management, single source of truth and reporting, 2) opportunity for 'challenge, build and support' business unit plans, 3) a focus on delivery to increase 'time to value,' 4) increase overall change capabilities. An additional benefit is to ensure that no type of Change (i.e., CapEx/Exceptional spend) has a 'back door' to short cut spend approval, benefits realisation or risk management. As stated earlier, the key is earlier intervention, transparacy and consistency. If this is not delivering results, as independently verified by IA, additional layers of assurance can be put in place.

6. In the medium term (9-18 months), the current organisational structure could be further optimised, including removing up to 5 FTEs (see **Appendix B6**) and possibly reducing the average cost of some positions. The ability to reduce costs and increase efficiency would be triggered by evidence of higher quality change management (e.g., improved prove/business cases, constant and consistent project management, etc.) and stable cross-portfolio management (e.g., high quality reports, a cross-portfolio delivery plan, managed resource constraints).

7. In the longer term, once the organisation can handle both simple and complex changes, the ultimate change goal would be to manage the change "organisation as an organism" with cross-functional teams using Agile methodologies and coaches possibly within re-aligned end to end business structures, internal strategy teams identifying continuous improvement opportunities, multiple 'speed of change' delivery models and processes, internal PO secondments for change delivery and ultimately fewer, bigger change portfolios.

8. While the longer term view may be 24 months away, it will be evident when:
    1. Change is consistently delivered on time, to cost, within risk profiles;
    2. benefits are fully identify and delivered, on time in full;
    3. the SPO can effectively manage a governance process, with forward planning;
    4. the business can appropriately resource change activity balance skills, speed, cost;
    5. and business units can create well thought out, written and articulated business cases and "go live" documentation

POL00423464

Risk, Compliance and Audit Report

Author: J Ellwood, J Hill, J Appel Sponsor: Al Cameron/Ben Foat Meeting date: 23 September 2019

Executive Summary

Context

This paper provides an update on the risks and compliance matters that Post Office is managing and an update on the latest Internal Audit position.

Questions this paper addresses

- What are the key risks and compliance issues and what is being done to address these?
- What are the emerging risks we face in both the short and medium term and what are we doing to address these?
- How is the Risk Framework maturing?
- What is the status of the Change Portfolio and its current top portfolio risks and key delivery challenges?
- What progress is made with delivery of the Internal Audit programme and completion of audit actions?

7

Conclusion

- The paper provides an update on the following top risks: PCI, Information Security, IT Technology & Interruption and Brexit.
- A Risk Register and Governance Framework are being developed with Payzone, informed through a workshop which took place in July with Payzone's Lead Team.
- Financial Crime team report a growing number of high volume and complex cases relating to Banking deposits as the Banking Framework volumes increase.
- The Ofcom text relay investigation continues where we are likely to face regulatory censure and a fine.
- Delivery of the Internal Audit programme is making good progress. There are currently 46 open audit actions, 1 of which is overdue.

Input Sought

The Committee are asked to note the revised Harm Table agreed at RCC, which is used to assess risk impact and probability (see par. 1.16). No other decisions required at this time.

POL00423464

The Report

Risk

Author: Jenny Ellwood

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

1.1 There has been minor change to the heatmap status (Appendix 2 within Reading Room). Legal and Regulatory and Strategic are the principal risk categories which continue to report Red and where there is continued focus on actions.

1.2 The latest position of the Top PO Risks is shown in Appendix 3, within the reading rooms. IT Technology and Business Interruption risk has increased from Amber to Red. This is as a result of the following: a) IRRELEVANT

IRRELEVANT

7

1.3 PCI remains an area of concern, a separate update is provided from the Programme. Whilst work with Ingenico continues the proposed solution, costs and timeline is expected in October. A trial of the updated pin-pads in model office is underway and Plan B alternative solutions continue to be explored, however, to date no improved designs have been established.

1.4 On IT Security Transformation Programme (ITSTP), all ten key recommendations from the Deloitte Cyber Maturity Assessment have now been completed and a separate paper has been provided by the CISO. This paper includes confirmation of the revised Cyber Risk Appetite and approach for business assessment and monitoring.

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

1.7 A comprehensive risk workshop took place at Payzone in July, it was well supported, with attendance from all the lead team. The session covered a full walkthrough of each area's accountabilities from product design and development, through to termination of an agent. A number of potential risks were discussed which will now be formally recorded within a risk register. This will be finalised ready for review at Payzone's Board at the end of September and will inform the internal audit scheduled to start late September.

1.8 In terms of Risk Governance, to align with the key areas of PO's risk framework, Payzone are looking to define their risk appetite and agree an approach to assessing risk in terms of impact and probability. Again, this is planned to be discussed and agreed in September's Board. Central Risk are continuing to support Payzone with this work.

POL00423464

1.9 Additionally, it has been confirmed that Payzone's Operations Director will take the leading position on risk management and has recruited a dedicated role who joined the team in August. This role will support him in risk and quality management.

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

1.10 A Board paper on Talent and Succession was presented and discussed in April 2019, and it was agreed that the identified Talent list needed to be expanded so that there were more names added to the list. The GE agreed to review the list of names to include a broader review of names which has been pushed out to later in 2019, once Nick Read has settled into the business.

1.11 The issue of retention of key individuals has been picked by the GE and is also being reviewed.

1.12 A risk has been raised relating to the Banking Framework, Barclays have notified PO that they will not accept new commercial pricing for Banking Framework 2. They have requested to reduce their overall exposure and have therefore notified PO that they will cease cash withdrawals through branches from January 2020. Whilst this is commercially driven, the customer and branch impact may see c.10% of cash withdrawals reduce during 2020.

1.13 The risk is that other banks may follow suit in 2021 or 2022, although unlikely bearing in mind the different strategies, cultures and branch estates sizes of the other banks. A PR campaign is being developed to mitigate the positon as part of the strategy for the Post Office, this will be launched mid-October. Whilst this is unlikely to change Barclays' decision, it may deter other banks (who may also benefit from migrating customers).

1.14 Brexit 'No Deal' planning continues. A review of the risks has been undertaken by the Lead Team and no new risks have been identified. The plans which were formulated and enacted in March have been validated and work is underway to agree a communications and delivery plan. The focus continues to be on changes required for Mails and the additional support we may need to provide to key branches. Fortnightly meetings are in place with BEIS. A detailed review took place on 4 September and they were happy with our preparations. We are also in discussions with the Government on how we could support communications to small businesses as the Government's activities to engage and communicate the impacts of a 'No Deal' to the UK continues. BEIS confirmed that even after recent government events that we should still work on mitigations required for a 'No Deal' scenario.

How is the Risk Framework maturing?

1.15 Work has been undertaken to review and refresh the Risk Management Framework. A single document has been developed to reflect current practices and will support the revised Risk Policy, which will come to committee for approval in November. A Risk intranet site is also under construction which will make all risk information more visible to the business.

POL00423464

1.16 Additionally, RCC members have reviewed and approved the revised Risk Impact and Probability Harm Table used to assess risk impact and probability. Language has been simplified and category on customers/postmasters added in. Key revisions made with stakeholder / SME feedback are shown in Appendix 4.

1.17 The development of the Archer Risk and Control application continues. User Acceptance Testing is planned for September, with full training of the Central Risk Team in October and we anticipate a technical go-live date of early November. There will subsequently be a phased migration of risk data by business area into the platform. Internal Audit have begun a review of the Archer implementation project to determine the extent to which current implementation plans follow technical best practice and meets the business requirements from the core risk team. The High Level Plan is shown in Appendix 1.

1.18 In terms of Change Risk a significant amount of work has been undertaken on implementing a Service Now module to support the management of change risks, assumptions and issues. The module went live in July. It allows all programmes/projects to manage their risks into a single on-line corporate repository rather than the previous manual process. The data is readily accessible (in real-time) not only to the Project Sponsor and Project teams but also to the Strategic Portfolio Office (SPO) and Change Risk & Assurance (CRA) teams.

1.19 The data migration activity continues at pace, which is enabling the creation of real time meaningful MI which will enable us to further improve our reporting packs for this committee.

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

1.20 The overall status of the portfolio remains Amber. Focus on activities to increase confidence in both overall and certain individual cost and benefits projections has continued. People risks continues to be the top risk reported. A separate update paper is provided by the Chief Transformation Director, which confirms the activities being undertaken to improve change maturity including training to strengthen people capabilities.

Compliance Author: Jonathan Hill

Telecoms

Text Relay

2.1 Ofcom has sent Post Office a second S135 information request, requesting primarily all documents we hold in relation to discovery of the issue, the reason why it occurred and what steps were taken to fix the issue. As this requires a search of all telco team emails Ofcom has granted us an extension to 12 September 2019 for these questions. Emails have been retrieved from our emails system and have been reviewed to identify those in scope of the request. Our response is being reviewed by legal counsel

2.2 We have a meeting with Ofcom on 24th September to discuss the response.

POL00423464

Regulatory Diary

2.3 The Telecoms Regulatory Diary is provided as supplementary information (Appendix 5).

Data Protection

GDPR Contract Remediation

2.4 Of the original 401 contracts, 88 remain to be remediated as at 11th September. Of these, 53 are material and of those, only 8 are high risk. The working group is reviewing the previous approach taking to remediation, to create a model which allows a more efficient remediation of the remaining contracts.

2.5 This will involve taking a stronger approach in our legal standpoint. The proposal is to initiate 'deemed consent' on low risk non-material contracts where the level of personal data being processed is negligible. This would potentially remediate over a third of outstanding contracts. This approach will only be used where we have made multiple (at least 3 attempts) to contact the supplier with no response.

2.6 It is anticipated that the remediation exercise will continue to March 2020.

Data protection breach

2.7 In line with the Post Office move to use Western Union for international payments, Post Office instructed Moneycorp to close all International Payments accounts on 31st July 2019. On 9th August, as part of that closure process, an email communication was sent to c. 130,000 customers informing them that their account was now closed and what would happen next.

2.8 Advice had been given that no marketing materials should be included in this communication, however, an advertising banner and email header marketing the new Western Union services offered by Post Office was included and the email was also sent to customers who had previously closed their accounts. The investigation is ongoing and we are currently awaiting the number of customers who received marketing emails when they had not given permission.

2.9 Currently we have received 10 complaints from customers, all of which came in on 10th August and have been responded to by the DP team. This is not a notifiable incident to either the data subjects or the ICO, although the ICO might take an interest should any customer decide to complain direct to it.

Financial Crime

Compliance with Money Laundering Regulations

2.8 Between 20th June and 5th September 2019, 132 new Bureau de Change non-conformance cases were identified in comparison to 112 during the same period in 2018. This increase is accredited to the improvements made to the Bureau de Change transaction monitoring system, and is expected to continue as we implement new reports.

POL00423464

2.9 Between 20th June and 5th September 2019, 29 non-conformance cases related to customers who had purchased in excess of IRRELEVANT in 90 days. Mitigating actions have been taken and the individuals have been reported to the authorities where required.

2.10 There were two material breaches in July and August. The first breach related to a customer purchasing c IRRELEVANT in foreign currency at IRRELEVANT different branches, at all times below the IRRELEVANT single transaction value threshold. The Financial Crime team identified these linked transactions and reported them to the NCA, having identified the customer as being deaf. All branches concerned were contacted and the activity subsequently stopped. The second breach was a customer who had exchanged c. IRRELEVANT over a 5 day period. The customer deposited the sterling amount into their bank account each time. Following contact by Post Office with the customer's bank there have been no further transactions.

2.11 The outstanding AML Credence architecture issues that are impacting Bureau de Change transaction monitoring are still being progressed by Accenture. The DCoE team are providing support to Accenture and expect the fixes to be complete by the end of September. Testing will then need to be undertaken by DCoE to ensure these that all outstanding issues have been resolved.

7

Anti-Bribery and Corruption ("ABC") update

2.12 To help reduce reporting errors, a review of the Gifts and Hospitality Tool has been undertaken and some updates have been made to the submission form and user guides.

2.13 Annual ABC training was launched on 6th September and has been enhanced with animations to help reduce errors.

Whistleblowing update

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

Fit and Proper

2.15 Gathering agent F&P returns continues and we are sharing data with HMRC fortnightly to evidence our progress, however the deadline of 23rd August to provide declarations has been reached:

- The Declaration Oversight Committee met on 28th August and formally approved the switch off of non-compliant branches. The impacted branches have been notified, as have external stakeholders (MoneyGram and FRES) and internal stakeholders (Supply Chain, NBSC, etc.).
- For all other agents, c.1,000 branches have had Travel Money and MoneyGram services switched off. System constraints necessitated data to be loaded in batches rather than in a single submission. The first batches carried a switch-off date of 6th September, the second (final) set of batches have an effective switch-off date of 13th September.
- These agents will continue to be contacted by Network Area Managers, and the F&P team in Chesterfield. Agents that achieve a compliant position will have their Travel Money and MoneyGram services switched back on - a switch-on batch will be processed once a week from w/c 16th September, for a period 60 days.

- Agents which remain non-compliant after that 60 day period will be de-registered from HMRC.

2.16 The next switch-off deadline will not be until Q1 2020. Processes and systems changes required for ongoing annual F&P declaration from January 2020 are being developed and agent annual declarations will be spread throughout each year.

2.17 A verbal update on the latest position will be presented at ARC.

Regulatory updates

2.18 The Foreign & Commonwealth Office have published guidance on how the UK would implement sanctions if the UK leaves the EU without a deal. If there is no deal, the UK will look to carry over all EU sanctions at the time of our departure. The Sanctions and Anti-Money Laundering Act 2018 will provide the legal basis for the UK to impose, update and lift sanctions after Brexit. This means there will be no gaps in implementing existing sanctions regimes if there's no deal.

External Threats

2.19 We continue to see a growing number of high value and complex cases relating to banking deposits. Between 1st May 2018 and 1st July 2019 there have been 46 investigations relating to partner banks; the total amount linked to these cases is c. IRRELEVANT Post Office is taking all reasonable actions to identify these transactions (which are anonymous to us) and raising SARs with the partner banks and law enforcement.

2.20 As a result, law enforcement agencies and the banks are now stepping up their investigations.

2.21 In July/August, HMRC presented 3 cases arising from SARs submitted by Post Office, totalling c. IRRELEVANT, to the UK's Joint Money Laundering Intelligence Taskforce ("JMLIT"), of which we are a member, highlighting evidence that cash derived from criminal activity is being placed over Post Office counters.

2.22 As part of the Banking Framework assessment and the growing volumes of cash deposits, we have sought external legal advice on the money laundering risks to both the MLRO personally and the Post Office. Whilst, from a regulatory perspective we are taking all reasonable actions and the main risk lies with the banks, Pinsent Mason has advised that IRRELEVANT t IRRELEVANT

- IRRELEVANT

2.23 These risks and potential mitigants are being considered as part of the current re-assessment work. This includes:

- Meeting with the Banking Team to explore additional actions we can implement with the banks to reduce this risk.
- Continue to raise awareness of placement risks in high risk areas, including working with the Area Managers and NFSP.

POL00423464

- As well as our own review into the risks, we have recently been approached by the National Economic Crime Centre and the Pro-Active Taskforce at the Economic Crime Directorate (attached to the National Crime Agency), to understand the migration of placement risks from banks to Post Office. We are working closely with these law enforcement agencies to assist them with these investigations and help mitigate the risk to the Post Office.

2.24 Reviewing sales of Lottery and Scratch cards to Vulnerable Customers: Ladbrokes Coral were fined £5.9m by The Gambling Commission for not protecting vulnerable customers and for failing in its anti-money laundering measures. Although Post Office has limited gambling products, it does highlight the importance of protecting vulnerable customers and our social purpose. Currently Post Office does not apply any limitation to the number of National Lottery and Scratch cards a customer can purchase over our counters and this will be reviewed when these products are next assessed

Supply Chain Compliance

2.25 Six audits were completed between June and August with 17 Improvement Needs identified, and a combined audit score of 35 which is in line with the national average. An external supplier audit was conducted on Premier Works (agency recruitment) with 1 Improvement Need identified. No recurring issues identified in internal or external audits. One key issue identified during the Glasgow audit related to CWC outward remittance functionality regarding the ability for clerks to re-print their own barcodes and this is being investigated by Supply Chain.

Financial Services

Credit Cards

2.26 Following the agreement with Capital One to provide credit cards we met the Compliance team of our new regulatory Principal.

2.27 We will be working together with Cap One to put in place a Regulatory Guidance Manual that outlines the key responsibilities Post Office has to put in place to maintain compliance, including financial promotions approval processes. Initially Cap One proposes customer digital marketing to begin before the end of the year.

Mystery Shopping Results

2.28 Branch Mystery Shopping results for July and August continue to show poor conformance to the Travel Insurance sales process, where colleagues are not giving the Eligibility and Medical Laminate to customers so they can confirm medical condition status. Specific training on Travel Insurance has been provided to align with the summer period and further refresher training on IDD is planned for Q3.

2.29 Video Mystery Shopping results for Savings have improved in August (7% reds), this is partially due to the Personal Loans journey being switched off on the CRM Tablet whilst updates are completed and further training is being rolled out for Savings. Life Insurance shops have improved in both July and August (average 7% reds over the 2 months).

POL00423464

CRM support structure

2.30 The CRM support structure is now in place with 4 Area Managers performing the role of Support Manager. POL Conduct Compliance is monitoring performance and providing support and guidance.

Vulnerable Customers

2.31 The FCA issued a guidance paper in July focused on the fair treatment of vulnerable customers. This focuses on the skills and capabilities of staff to support vulnerable customers, how customer processes react to the vulnerability challenge and how firms monitor how well they perform.

2.32 So far, the guidance consultation - which is to be given in two parts - was not as prescriptive as initially feared. We will work with our Principals on understanding if we need to make any changes to processes in how we support vulnerable customers and whether we respond to the first consultation by October 4th.

2.33 The Post Office Vulnerable Customer Policy has been refreshed with some minor reference changes and is the reading room for annual re-approval. The Policy was recently reviewed by an external accessibility expert Kate Nash Associates who support that the policy meets all the expected requirements.

Regulatory Diary

2.34 The FS Regulatory Diary is included in the supplementary information as Appendix 6.

Supplementary information

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

- Right to erasure requests (Appendix 7);
- Compliance dashboard (Appendix 8 & 9).

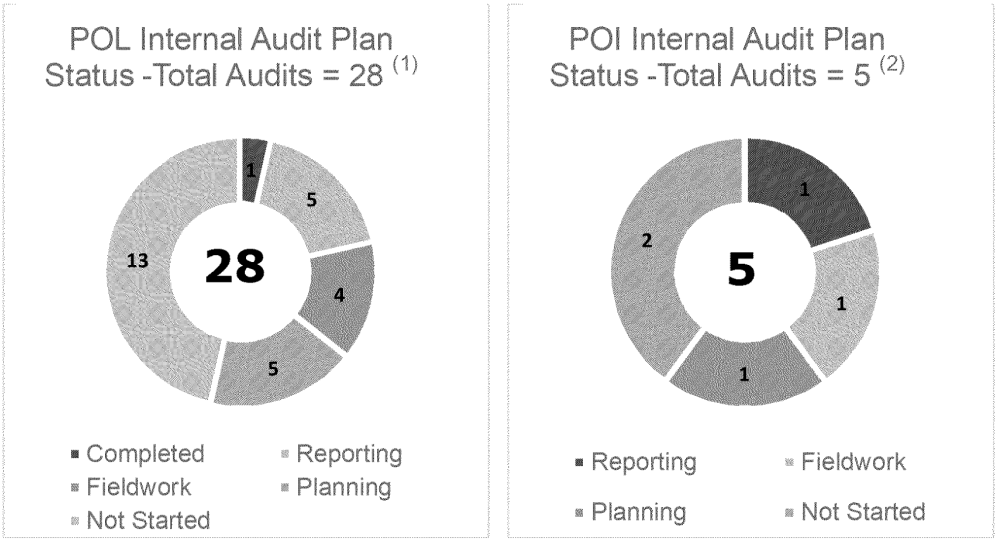
Internal Audit Author: Johann Appel

Progress against plan

3.1 Delivery of the 2019/20 programme is making good progress, although no additional audits were finalised since the July ARC meeting. This was mainly due to the summer holiday season impacting the availability of Post Office employees and Deloitte staff. Nine in-flight audits are being scheduled for reporting at the November RCC and ARC meetings (7 POL and 2 POI).

POL00423464

3.2 Current delivery status is as follows:



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

(2)POI ARC approved baseline plan for 2019/20 (5 internal audit reviews).

7

Internal Audit reviews in progress and planned

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

Post Office Ltd			
	Review	**Status**	**Timing**
1	Procure to Pay	Final report for Nov RCC	24/06 – 15/08
2	Data Analytics Excellence (Change)	Final draft report for GE comment	12/06 – 12/08
3	Effectiveness of Gating Ph1 (Change)	Draft report	12/07 – 16/08
4	Effectiveness of Second Line Assurance Ph1 (Change)	Draft report	12/07 – 16/08
5	Benefits Realisation Ph1 (Change)	Draft report	12/07 – 16/08
6	SGEI Reporting	Fieldwork	12/08 – 20/09
7	Employee Expenses Follow-up	Fieldwork	26/08 – 30/09
8	Payzone Internal Controls 'Health Check'	Fieldwork	23/09 – 15/10
9	Archer Implementation	Fieldwork	09/09 – 27/09
10	Payment Technology Upgrade (Change)	Planning	23/09 – 15/10
11	Digitising Mails (Change)	Planning	Oct
12	Telco Billing Process	Planning	Oct
13	CFS Controls	Planning	Oct

Post Office Insurance			
1	Change Capacity	Reporting	21/08 – 09/09
2	Nemesis Programme Assurance	Fieldwork	21/08 – 13/09
3	Oversight of Third Parties	Planning	Nov

SGEI Reporting

3.4 The Board is required to approve the 2019 Network Report and confirm compliance with the Entrustment Letter and Funding Agreement with respect to SGEI provision as at March 2019. Internal Audit have been asked to review the SGEI validation process to support the Board in this.

3.5 The internal audit work to date has not identified any areas of concern that would result in the level of assurance provided to UKGI being overstated. A summary report of our findings and conclusion will be circulated during the meeting.

Status of Audit Actions

3.6 Audit actions are generally being completed on time. As at 13 September 2019 there were 46 open actions, 1 of which was overdue.

Audit Action Status:	**POL**	**POI**	**Total**
Open (not yet due)	36	9	45
Overdue (<60 days)	0	0	0
Overdue (>60 days)	1	0	1
Total	37	9	46

3.7 Following is a summary of the overdue action and latest status update:

Description of audit finding and Priority rating	**GE owner and due date**	**Action Owners and Status Update**
Payzone Acquisition and 100 day plan		
The execution of the Day 1-100 did not deliver the envisioned business objectives (specifically MSA and TOM outstanding) **(P1)** **Action:** Payzone MD will formally agree a MSA with Post Office and will complete the bill payments TOM.	Debbie Smith 30/06/2019	**Owner:** Andrew Goddard MSA has been agreed and is pending final signature (expected by 17/09/19).

END OF REPORT

POL00423464

Post Office Insurance Renewal

Author: Mark Dixon Sponsor: Al Cameron Meeting date: 23 September 2019

Executive Summary

Context

The business has a series of insurance policies due for renewal on 1 November 2019.

Question addressed in this report

How do we know that the programme cover we have in place is appropriate (i.e. the risks that are being insured, the indemnity limits etc.)?
How do we know that the overall cost of the programme is optimal for POL (i.e. the trade-off between claims paid, deductibles, claims retained, premium paid etc.)?
What features of the programme have we changed this year compared to the November 2019 renewal and why?
Are there any material gaps that were identified that we've decided not to cover that the ARC should be aware of?
What specific work have we performed around cyber?
What is the proposed programme structure and cost at 2019 renewal for approval?
How can the ARC be sure that we have disclosed all material facts to insurers?

8

Conclusion

1. A summary of the policies and cover in place at renewal in 2018 is included as Attachment 1. With the exception of cyber, where we are increasing our coverage, insurances to be purchased are broadly the same as last year. For cyber, given the increased severity of attacks and that the current IRRELEVANT is an aggregate limit across the various covers, we believe that an additional IRRELEVANT of cover (i.e. an increase to IRRELEVANT would be prudent.

2. We have changed our approach to the renewal process this year. We are in the process of completing an OJEU-compliant procurement for the 2020 renewal. In addition, we have worked with IRRELEVANT, our broker, to perform a detailed risk

POL00423464

review to identify potential gaps in coverage. The output was used to adjust coverage where appropriate. All significant changes are outlined in this paper.

3. Our insurance programme covers the business for most major risks albeit with high deductibles. As a result of our changed approach to renewal in 2019 we have been able to make reductions in these deductible levels. We consider these levels of insurance to be reasonable and appropriate for the POL business.

4. POL has not made any claims against its insurers over the last year largely due to the significant levels of self-insurance (via deductibles).

5. The annual cost of insurance in 2018/19 was circa IRRELEVANT We are finalising the cost for 2019/20. We will make savings on lines procured through the OJEU process but expect these savings to be offset by higher premiums on Crime and D&O policies. Absent the changes to cyber we would expect cost to be broadly in line with last year. The increased cyber cover is likely to increase premium by approx. IRRELEVANT

6. We believe that the change in approach adopted for the 2019 renewal allows us to conclude that we have appropriate coverage in place, with appropriate deductibles, at an optimal cost for POL. For 2019 we will achieve this with an OJEU-compliant process.

Input Sought

The ARC is asked to approve the 2019 renewal on the basis set out in this paper and to authorise the Chief Financial and Operating Officer to agree any points required to finalise the renewal.

POL00423464

The Report

How do we know that the programme cover we have in place is appropriate (i.e. the risks that are being insured, the indemnity limits etc.)?

1. We work with a respected broker who knows our business. IRRELEVANT were appointed as insurance broker to the Post Office in 2015 and have now worked with POL on its 2015, 2016, 2017 and 2018 renewals. They have helped achieve premium reductions of c.15%, c.18% and c.3% in 2015, 2016 and 2017 respectively, as well as various improvements to our policies.

2. We ensure that the interests of the broker are contractually aligned to ours. During 2019 we extended our contract with IRRELEVANT. Under the new contract they are incentivised to ensure costs to POL are minimised.

3. With the help of IRRELEVANT we have performed a detailed risk review and gap analysis. We've identified material risks to the business from the risk register; we've identified which of those risks are insurable; we've identified what we've actually insured; we understand the insurance products available; and we've therefore identified the areas of our risk profile that are currently insured adequately and where we have gaps in our insurance coverage. From the tender process (or from estimates provided by our broker) we've obtained sufficient financial information to price what it would cost to close these gaps.

4. We believe that we've therefore made appropriately costed decisions around coverage.

How do we know that the overall cost of the programme is optimal for POL (i.e. the trade-off between claims paid, deductibles, claims retained, premium paid etc.)?

5. Where claims volumes are at a level that allow it, our brokers have performed statistical analysis of "claims" incurred to assess the optimal self-insured retentions (deductibles) and used this knowledge in our invitation to tender. We've tested the market for pricing of deductibles at different levels. This has allowed us to identify the level at which insurer pricing models and our appetite for risk produce the most economically attractive programme costs. Where claims volumes are insufficient to allow such analysis, we have used our broker's knowledge of insurer pricing models and appetite to identify deductibles that produce the most cost efficient policy structures. Our broker has good knowledge of the market and their interests are contractually aligned to ours.

POL00423464

What features of the programme have we changed this year compared to the November 2019 renewal and why?

6. Coverage for cyber will be extended from IRRELEVANT, see below.

7. For Motor, Employers Liability and Public Liability policies, we will renew based on a reduced IRRELEVANT any one claim deductible as well as a reduced combined aggregate of IRRELEVANT.

8. For our Property Damage & Business Interruption we will extend cover so all small locations (less than insured value of IRRELEVANT are additionally insured in the event of a natural catastrophe event impacting a wide area, with an additional premium of IRRELEVANT (total renewal premium IRRELEVANT.

9. We are exploring increasing the POMS indemnity limit under its Professional Indemnity policy from IRRELEVANT and will conclude upon this as we continue through the renewal process.

Are there any material gaps that were identified that we've decided not to cover that the ARC should be aware of?

8

10. The review broadly concluded that the level of insurance in place is reasonable and appropriate for the business.

11. Some gaps were identified around cyber and property where we have taken the opportunity to increase coverage.

12. There were two areas highlighted where we have concluded that the likely impact is within our risk appetite and have chosen not to take cover for this renewal, Key Person Insurance and reputation insurance, but will continue to explore for next year.

13. In addition, IRRELEVANT also highlighted the risk of impersonation fraud (social engineering) that could be covered under our Crime policy. As part of the Crime renewal we will obtain quotes and then conclude on the appropriateness of this cover. The final decision will be with the CFOO.

What specific work have we performed around cyber?

14. We have reviewed our existing Cyber policy to: a) ensure that it would respond as expected in the event of an incident; and b) conclude whether the sum insured, which is currently IRRELEVANT in aggregate for the year, is appropriate.

POL00423464

15. The policy would respond in the event of an incident but the amount covered is low given the increased interest in data loss from regulators and the increase in severity of attacks. We are therefore proposing to increase cover from IRRELEVANT to IRRELEVANT. Our brokers estimate that the increased coverage will raise the premium from IRRELEVANT

16. Much of our IT activity is delivered by third-party vendors, primarily IRRELEVANT IRRELEVANT Our expectation is that, in a cyber event, we would be heavily reliant upon responses by these vendors. The starting point for the review work was therefore to provide our brokers with a detailed understanding of how we protect our network, what measures suppliers are applying to protect us, and where different responsibilities lie. The work that was performed, i.e. asking vendors to declare the end-to-end security defences that they have in place to protect Post Office, together with other details of our layered security defences, was shared with the Cyber team at IRRELEVANT

17. We then worked with IRRELEVANT to look at the impact that three recent cyber incidents would have had on the Post Office. The three incidents were:

British Airways – the loss of customer data through a fake booking website resulting in an ICO fine of £183m;
Marriot Hotel Group – the loss of data through an acquired company – 300 million customer records extracted – resulting in an ICO fine of £98M; and
Morrisons – a disgruntled employee extracting colleague payroll data and publishing it on the web – resulting in a 'class action' and significant damages expected

18. We concluded that POL would be covered for the costs to get 'back to normality' under all three scenarios. It should be noted that a company cannot insure against fines and penalties.

19. The back to normality costs cover three buckets of activities:

Breach response costs: e.g. IT Forensic experts, customer / business communications, PR agency advice, Experian credit checking costs, legal advice and notification to the ICO;
Liability coverage: e.g. Privacy style class action costs including legal costs, noting however, it does not cover any breach fines; and
Business interruption: e.g. loss of income (this includes system / outages not just cyber related), standing up of bespoke call centres for customers.

20. Given the increased severity of attacks and that the current IRRELEVANT s an aggregate limit across the various covers, we believe that an additional IRRELEVANT of cover (i.e.

POL00423464

an increase to IRRELEVANT would be prudent. Most costs are likely to fall into the breach response and business interruption buckets. However, where breaches involve a large number of customers and their data then we cannot rule out the risk of privacy class actions. For example, the Morrisons class action is estimated to cost IRRELEVANT in addition to response and business interruption costs.

21. It should be noted that, given our IT arrangements, certain costs are likely to be incurred by suppliers and therefore would need to be either met directly by the supplier or out of its insurance cover. For example, it is more likely that IT forensic experts would be required to be deployed within a supplier's organisation and hence the cost would be for the supplier and not covered by POL's insurance. Further, the large costs associated with the cases described above (BA, Marriot Hotel Group and Morrisons) were largely related to fines from the ICO which cannot be insured, although the incidents also generated substantial costs for the organisations involved which would have been covered by a cyber policy.

22. Given the above, it is important that strong contractual remedies are in place with critical vendors and that our vendors have adequate insurance in place to cover a cyber incident. The vendor's cover should support any policy we have. We have asked the question of our four key vendors, i.e. IRRELEVANT IRRELEVANT and received positive confirmation from each supplier. It should be noted, however, that more work will be carried out in this area and, where necessary, contractual obligations reassessed and negotiated during review periods.

8

What is the proposed programme structure and cost at 2019 renewal for approval?

23. The structure for renewal is still being determined but will be largely as per the existing structure. A structure chart, showing IRRELEVANT recommendations, together with current expectations around premiums is attached as Attachment 2. We will be looking at some changes to deductibles as detailed above IRRELEVANT

IRRELEVANT

24. The premiums and deductibles stated within the attached programme chart and premium table are based on IRRELEVANT recommendations for the upcoming renewal. As mentioned terms for a number of lines are still being discussed and therefore premiums and the insurer names are not yet available.

25. Whilst the OJEU tender process worked well for Property, Motor, Employers Liability, Public Liability and Personal Accident and Business Travel insurances, as expected we received no OJEU responses for the following lines of insurance and

POL00423464

as such are able to utilise normal 'open market' tendering processes and these are underway: IRRELEVANT

26. Because of the state of the Crime and D&O markets we expect premium increases. Insurers will also not fix pricing for these lines until 30 days prior to renewal.

27. The annual cost of insurance in 2018/19 was circa IRRELEVANT, excluding IPT. We are finalising cost for 2019/20. We will make savings on lines procured through the OJEU process but expect these savings to be offset by higher premiums on Crime and D&O policies. Absent the changes to cyber we would expect cost to be broadly in line with last year. The increased cyber cover is likely to increase premium by approx. IRRELEVANT It should be noted that the rate of IPT is IRRELEVANT.

How can the ARC be sure that we have disclosed all material facts to insurers?

28. Post Office have worked with its insurance brokers to ensure the 'search' process, the people within the business consulted and the breadth/depth of information gathered is consistent with our duties under the Insurance Act. Our insurers are aware of and familiar with our disclosure processes and are comfortable with them

29. The process has been in place for a number of years and was enhanced post-Insurance Act, so is well tried and tested

30. We have built long term, consistent relationships with insurers, which helps with the development of their knowledge and understanding of our business (with consequential benefits in terms of disclosure risks).

31. However, whilst we have robust procedures in place it is not possible to give 100% certainty in this area. Our insurances do give some help in this regard:

32. Our property insurance policy provides an element of cover for 'inadvertent omissions'.

33. Our brokers review our policy wordings and seek to remove where possible onerous conditions and warranties that might impact coverage should non-disclosure occur.

Attachment 1: Summary of Insurance Programme at 2018 Renewal

Attachment 2: Structure Chart and Premium table showing IRRELEVANT Recommendations for the 2019/20 Renewal

8

POL00423464

Policy Summary Paper

Author: Elizabeth Adams Sponsor: Jonathan Hill Meeting date: 23rd September 19

Executive Summary

Context

This paper provides a summary of changes that have been made to the policies in section 5 of this report as part of their annual review process for the Audit, Risk and Compliance Committee to consider and approve.

Questions addressed in this paper?

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

Conclusion

3. In order for Post Office to maintain its policy governance responsibilities owners need to review their policies regularly.
4. The Post Office is compliant with the requirements of the Modern Slavery Act 2015 in terms of its legal obligations. It has made progress in defining what needs to be done across the business and is beginning the longer term task of robust implementation. Post Office has prepared a new Statement for 2019/2020 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end. There are measures in place to ensure it will be published online on or before **30th September 2019**.

Input Sought

The Committee is asked to review and approve the updated Policies and the 2019/2020 Modern Slavery Statement and endorse the proposed actions for the business to take these forward.

POL00423464

The Report

Which policies were updated in this annual cycle review?

5. In this review cycle **7** policies were revised and require ARC approval. All policies (apart from the Modern Slavery Statement) can be found in the reading room.

Policy	Last Reviewed	Updates
Modern Slavery Statement	2018/2019	Annual Review statement must be published by 30 Sep 2019
Contract Execution Policy	n/a	New Policy
AML & CTF Policy	October 2018	Minor updates made
HMRC Fit & Proper Policy	October 2018	Minor updates made
Physical Security Policy	April 2016	Minor updates made
Financial Crime Policy	October 2018	Minor updates made
Vulnerable Customers Policy	October 2018	Minor updates made

What updates were included and why?

A summary of the changes/updates is below:

Modern Slavery Statement

1. Our 2019/2020 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2019/2020.
2. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Progress in 18/19 was mostly in supply chain areas, and in 19/20 focus is more on network as MS sponsorship has moved to the Retail Director and as highlighted, the majority of the risk sits in the Network. Our commitments in 2018/19 were to raise awareness of Modern Slavery across our supply base and agency network, and provide training and educational pieces to the field teams.

POL00423464

Contract Execution Policy

3. This new policy sets out the appropriate methods of contract execution in the Group and the controls required for each method. It also enables e-signatures to be used within the business. A Quick Reference Guide has also been produced to summarise the policy so that it is more accessible to the business. The policy therefore tightens the controls around contract execution, ensuring reliable methods of execution are used whilst still offering a practical solution for the business.
4. The acceptable forms of e-signatures are outlined in the policy in paragraph 1.5.2.
5. Deeds may not be signed electronically and the methods of execution of deeds are set out in paragraph 1.5.3 of the policy.

Anti-Money Laundering & CTF Policy

6. There has been no legislation changes in the past year.
7. Clarifications have been made in relation to core principles and methodology.
8. Minor amendments have been made in relation to the definition of the offence of 'Tipping Off'.
9. A risk based approach is being adopted for product and service financial crime assessments, to support the business and product managers, and ensure the Financial Crime team can support critical business delivery timescales.

HMRC Fit & Proper

10. We have amended the HMRC Fit & Proper policy so that it is in the format of a policy standard supplemental to the AML/CTF policy, and moving forward will only require RCC approval.
11. The creation of the Declaration Oversight Committee oversees that the agent population meets the requirements of the fit and proper.
12. New Direct Employee List changed to reflect organisational changes within last 12 months.

Physical Security Policy

13. Minor changes made to the minimum control standards, specifically 'prevention controls' to ensure clarity to enable measure / testing.

Financial Crime Policy

14. There has been no legislative changes within the past year, only minor amends have been made.
15. Additional minimum controls to deter, prevent and detect financial crime and fraud by employees to reflect practice, ensure transparency and bring into assurance checking regime have been included.

Vulnerable Customer Policy

16. There has been no significant legislation changes in the past year.
17. A new vulnerable customer training module has been introduced on success factors this year to accompany the policy.

POL00423464

Modern Slavery Act Statement

Author: James Scutt Sponsor: Amanda Jones Meeting date: 23rd September 2019

Executive Summary

Context

At the request of the Audit and Risk Committee in July, the Modern Slavery (MS) paper returned to the Risk and Compliance Committee with some more detail included in the report around progress. The additional information is highlighted grey.

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

Questions addressed in this paper

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

Conclusion

In order to give Post Office an independent and balanced view of its compliance to the requirements of the Modern Slavery Act, we employed the services of an external body of expert consultants with particular skill and knowledge in Modern Slavery.

10

Overall the Post Office is compliant with the MS ACT 2015 in terms of its legal obligations. It has made progress in defining what needs to be done across the business and is beginning the longer term task of robust implementation.

- Post Office has prepared a new Statement for 2019/2020 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end.
- The steering group has made progress and will continue to evolve with a full review of its terms of reference going forward.
- Due to the lack of control over operations in this area, the highest level of risk continues to be within our Agency Network but we have also identified several more areas where proximity of brand also poses a risk for Post Office. (When the Post Office branding appears on retail packaging, sourced by one of its suppliers)
- Published company statements on modern slavery face scrutiny from the media, pressure groups and the public. As an organisation with a reputation of trust and a stated social purpose, we consider it important for Post Office to demonstrate a clear commitment.

POL00423464

Civil society would expect the Post Office to be a champion in this area because of this trust legacy.

- Good Values recommends that Post Office increases its resources to be comparable to other companies of its size, however we believe tracking of MS activity can be effectively managed across existing resources.

Actions for 2019/20:

- Implement a new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.
- Review our supply base retrospectively by applying the focus of our new IT tracking system.
- Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.
- Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.
- Deploy specific MS awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.
- Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.

Input Sought

The ARC is asked to **RECOMMEND** the 2019/2020 Statement for Board approval and to endorse the proposed actions for the business to take forward in the 2019/2020 financial year.

Input Received

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

10

The Report

Why do we need Modern Slavery Act Statement?

The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36 million. It will therefore not apply directly to Postmasters if their annual turnover is less than £36 million. As Postmasters are part of the Post Office supply chain, Post Office must state what steps it has taken to ensure that it mitigates the risk of slavery and human trafficking in any of its supply chains or its business. Payzone has a turnover of just under the threshold so is not legal ly required to produce a separate MS Statement, best practice would be to do so and this is something we may want to consider. PZ will still be included as a business owned by the Post Office.

Post Office is required under s.54 of the Act to produce an annual slavery and human trafficking statement listing the steps taken to ensure its business and supply chains are slavery free. This paper attaches the third Statement (Appendix 1) which records what steps we have taken in 2018/2019 and outlines the actions we commit to take in 2019/2020. The Statement must be approved by the Post Office Board and signed by a Director.

POL00423464

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

Our 2018/2019 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2019/2020. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Progress in 18/19 was mostly in supply chain areas, and in 19/20 focus is more on network as MS sponsorship has moved to the Retail Director and as highlighted, the majority of the risk sits in the Network. Our commitments in 2018/19 were:

- Raise awareness of Modern Slavery across our supply base.
  - We referenced modern slavery in our terms and conditions for suppliers, ensuring that the requirement for compliance is understood and visible to our supply chain.
- Improve the due diligence assessment for onboarding new suppliers to our systems.
  - In 18/19 our Supplier Code of Conduct was introduced into the supplier onboarding due diligence process and we published this on our external web site. This can be found in Appendix 2.
  - Preparation work was completed internally to improve our data, design questionnaires and an evaluation scheme for supplier audits. This has enabled assessments to be completed in 2019/20 on suppliers and the risk assessment of our supply chain. There were 6 formal pre-qualification questionnaire (PQQ) exercises in 18/19 in which the MS evaluation appeared for 184 suppliers.
  - All our formal tender exercises use the Cabinet Office standard questions which include Modern Slavery was completed on all tenders in 2018/19
- Raise awareness of Modern Slavery across Post Office, its suppliers and within the agency network.
  - We completed an audit in July 2018, on "Premier Works" a company that supply CVIT staff to Post Office Ltd Supply Chain, with an outcome rating of Satisfactory.
  - This audit covered some key ACS Indicators relating to due diligence and labour provider requirements. It provided assurance the compliance controls for the vetting and recruitment of agency staff were working effectively. Two improvement needs were identified with a completion date by 09/10/2018 the actions related to Criminal Record Checks (CRC) and Financial Checks.
    - There was no evidence of financial checks conducted for 4 employees
    - There was no evidence of a Criminal Record Check for 1 employee only a receipt of a submission for a CRC, also CRC for 1 employee was outdated at commencement of employment. The employee commenced employment April 2018 the CRC was January 2017.
  - Actions have been taken to correct the findings and processes tightened to ensure future compliance.
  - Premier Works Support do not turnover more than 36 million so a slavery and human trafficking statement is not required. The 19/20 audit of Premier Works took place on 20th August. The audit went well with only 1 action relating to some gaps in personal files and no issues with RTW in UK or modern slavery checks.

- Educate field teams out in the agency network on spotting the signs of Modern Slavery.
  - Preparation was put in place to enable the deployment of mandatory Modern Slavery training to our Retail Field Team. This training has been deployed this year.

POL00423464

  - The MS Training has been allocated to 289 colleagues in Retail, these teams are specifically in roles who actively support our branches. 211 have completed with 78 yet to do so.
- Review our supply base and revise our supplier management processes.
  - Improvements captured in the above statements.

In formulating our commitments for 2019/2020 we engaged subject matter experts, "Good Values" to fully review Post Office's exposure to risk and approach to MS.

Good Values are a leading corporate responsibility and sustainability consultancy with over 10 years' experience working globally with corporates, NGOs and government departments. They help organisations manage the risks and exploit the opportunities from social and sustainability issues.

Good Values highlighted the main areas of risk to be:

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

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

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

No Dedicated Resource to be able to implement robust monitoring and due diligence, dedicated resources would need to be allocated to Modern Slavery to oversee the implementation across the business. Good Values highlight that, for an organisation of comparable size, our allocated resource is low.

What are the implications for the board and the business?

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

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

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

We are confident that the detail in our 2018/2019 statement recording our progress on last year and our proposed actions for the financial year 2019/2020 are appropriate. We will monitor developments, and keep the adequacy of the Statement under review.

POL00423464

Is the Post Office compliant with the Act?

Overall the PO is compliant with the legal obligations of the MS Act.

To establish the level of monitoring and due diligence within the Post Office that would be expected by civil society and stand up to public scrutiny, further focus and resource is required. Overall the Post Office is compliant with the legal obligations of the MS ACT 2015. It has started to make progress within the business, but it has yet to: embed training with employees; address the risk evaluation of our Postmasters and Agency businesses; conduct the required level of mapping and risk assessment with suppliers as set out in the Statement.

POL00423464

Modern Slavery

Appendix 1

1. Modern Slavery Statement 2019/2020

MODERN SLAVERY ACT TRANSPARENCY STATEMENT 2019/20

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

This statement is made pursuant to section 54(1) of the Act. It sets out the steps taken by Post Office & POMS during year ending 31st March 2019 to mitigate the risks of modern slavery and human trafficking in its business and supply chains.

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

This is the third statement in which we report on our efforts to mitigate the risks of modern slavery in line with the requirements of the Act. Our history has seen us focus on the rights and wellbeing of the people who work for Post Office and for our suppliers for many years. Our statement provides details of our policies, our approach and the actions we have taken in the 2018/19 financial year to strengthen our programme and commitment to respect and uphold people's fundamental rights and freedoms.

OUR BUSINESS AND SUPPLY CHAIN

10.1

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

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

Post Office directly controls around 2% of the Network of branches which consumers will generally recognise as the larger branches often situated in the centre of towns and cities across the UK. The remainder of the branches are managed on an agency basis by independent small retailers and shop owners operating Post Office services within their own store. Business owners may own more than one shop operating Post Office services and have a range of other non connected business interests. We also have agent managed facilities within some larger high street commercial partners, who like the smaller independent retailers, provide their own trained and friendly staff to provide our Post Office services to consumers.

POL00423464

Banking services

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

Postmasters

Postmasters can operate one or more branches. As agent's they have full control over how their branches within their retail premises are run on a daily basis. All those working in an agency Post Office branch are employed directly by the retailer. The Retailer is self-employed and typically takes on a Post Office as a valuable community service provided within their own retail business. Post office has no direct control over the operation of these independent SME businesses but does have the ability to influence and inform. Post Office aims to support Postmasters with their Post Office operations and influence their behaviours.

Commercial partners

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

Trade Unions

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

Third Party Suppliers

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

OUR BELIEFS AND PRINCIPLES

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

OUR POLICIES

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

CODE OF BUSINESS STANDARDS
We have a Code of Business Standards which underpins everything we do. The Code is mandatory and extends to everyone directly employed by Post Office. It requires all of us to act

POL00423464

ethically and comply with legal requirements at all times, putting our principles into practice in everything we do. The Code of Business Standards was updated during the 2017 financial year to include references to Modern Slavery.

WHISTLEBLOWING

We operate a Whistleblowing Policy so that all Post Office employees know how to raise concerns regarding wrongdoing or dangerous practices. The policy was updated during the 2017 financial year to include references to concerns about Modern Slavery.

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

RECRUITMENT & ONBOARDING POLICY

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

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

Post Office/POMS employs solely within the UK.

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

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

IDENTIFYING, ASSESSING AND MANAGING RISK

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

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

POL00423464

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

GOVERNANCE

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

TRAINING

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

WHAT DID WE DO THIS YEAR?

Proposals from 2018 Statement	Progress on 2018 proposals
Improve the due diligence assessment for onboarding new suppliers to our systems	We carried out a detailed assessment of our new supplier on-boarding process and identified a number of recommendations which will help ensure a robust assessment of new suppliers and their ways of working.
Review our supply base and revise our supplier management processes	We have designed an enhanced process and detailed content to be included in new system described above. Our CSR questionnaire is being trialled with a small cross section of suppliers, to test, review and make improvements to the question format, evaluation process and feedback/ improvement plan. We have aligned this with Post Office Compliance and Audit functions who conduct physical audits of Supply Chain suppliers. This ensures maximum benefit from our efforts and no duplication, or overburdening of the suppliers.
Raise awareness of Modern Slavery across our supply base	We created our Supplier Code of Conduct and published it on our public website. http://corporate.postoffice.co.uk/our-suppliers This Code of Conduct is used in the on-boarding process and other procurement exercises. Depending on the outcomes of the CSR questionnaire, we will devise additional awareness material as appropriate and distribute to our suppliers proactively.
Raise awareness of Modern Slavery across Post Office, its suppliers and within the agency network.	We issued guidance and Modern Slavery awareness raising material for Postmasters through our branch Network management teams and communication channels.

10.1

POL00423464

Educate field teams out in the agency network on spotting signs of Modern Slavery.	We sourced best practice training and awareness materials from suppliers and developed it to align and resonate with our Branch network management field teams. We will start to roll this training out to frontline staff.

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

As part of our initiative to identify and mitigate risk throughout 2019/20 we are committed to:

- Implement our new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.
- Review our supply base retrospectively by applying the focus of our new IT tracking system.
- Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.
- Continue to raise awareness of Modern Slavery across Post Office branch network across both directly managed and agency branches.
- Deploy specific MS awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.
- Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.

REMEDIATION PROCESSES

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

10.1

Post Office's Whistleblowing Officer: whistleblowing[GRO]k or by telephone on [GRO]
[GRO]
The Government's Modern Slavery Helpline or [GRO]

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

REVIEW

This statement shall be reviewed and published annually.

POL00423464

Compliance Report – Quality of Financial Services Sales in the Network

Author: Jonathan Hill/Amanda Jones Sponsor: Ben Foat/Debbie Smith Meeting date: 23 September 2019

Executive Summary

Context

Post Office is the Appointed Representative of Post Office Insurance (POI), Bank of Ireland (BoI) and, most recently, Capital One. As firms directly regulated by the FCA, each of these companies act as our Principal and are accountable for our conformance with the sales and marketing regulations of their FS products. We are subject to their oversight and supervision for FS products distributed through our sales and marketing channels.

Post Office has been selling and marketing these products through our channels in various ways since 2004, at all times subject to the sign off and monitoring by the principals.

Questions this paper addresses

1. Which FS products are sold and marketed through our channels and how is this done?
2. What are the Conduct standards we must meet?
3. What controls and supervision do we apply to provide Post Office and our Principals assurance that we are conforming to the regulations?
4. How are we performing?
5. What actions have we taken and are putting in place to achieve and maintain conformance across the network?

11

Conclusion

There are working controls in our Network distribution for Financial Services. The recent Internal Audit Review of Training and Competence has demonstrated the core T&C controls working. Core compliance training on Financial Services and Insurance train out how not to 'advise' customers and to ensure we treat them fairly.

POL00423464

Our monitoring MI shows that instances of mis-selling, pressure sales, cancellations and complaints are very low. What mystery shopping tells us is that we are weaker in consistently demonstrating the ability to follow the introductory sales process. This in itself could lead to poor customer outcomes, for example, customers may not be insured for medical conditions on travel insurance if they have not been asked the appropriate medical screening questions.

This emphasises the importance of keeping Network processes simple and easy to follow as well as ensuring we improve the understanding of Postmasters on why these processes are important for both the customer and compliance. The actions identified in the paper show how we are addressing this.

Our regular monitoring and MI is regularly reported to our Principals at the monthly conduct review Committees (Customer and Conduct Risk for BoI and Joint Conduct Compliance Committee for POI) where action plans are agreed and executed. In areas where risks have breached risk appetite we can and do suspend activity (see personal loans on tablets below).

Input Sought

The Committee is requested to note this paper

Report

Sale of Financial Service products

Financial Service products are distributed through the Branch Network, Contact Centres and the internet including the Post Office website.

At branch level, financial service products are primarily available through the DMB and Mains branches with Locals models offering products by exception. Branch products available over the counter include, savings accounts, travel insurance and over 50s life cover (current accounts and credit cards are currently withdrawn pending Peregrine transformation). There are also c130 Customer Relationship Managers-either Postmasters or their assistants- that also introduce life insurance, over 50s life cover and personal loans to customers via a digital tablet.

Branches are also an important source of lead generation capture for our other channels and an effective channel to make customers aware of other products on offer, e.g. mortgages, life cover and other domestic insurances such as motor, van, pet and home that are sold via call centre or internet.

The branch sales journey trained is always an introductory one and non-advised. So that customers can make an informed decision themselves on whether the product is right for them. For some products such as Over 50s life cover or savings accounts applications these can be completed in branch: for other sales

POL00423464

journeys such as loans or life insurance the customer is signposted to the call centre or website where they can complete their application journey.

- Directly Managed branches offer the full branch range of products to customers, this includes introduction and completion through Horizon where appropriate and lead generation;
- Agency branches offer varying levels of service:
    - Mains branches offer the full range of branch products to customers including the introduction and completion of a sale through Horizon. The majority of these branches would have leaflets and where appropriate, application packs.
    - Local models do not have leaflets or application packs and in the main do not sell Financial Service products, however there are exceptions to this rule with some branches selling Travel Insurance. The revised Retail strategy will see more of these branches being given the opportunity to sell more financial service products where it is deemed to be appropriate to meet customer demand and the Agent satisfies training requirements.

Training and Competence (T&C)

FCA has principles for the sale of financial service products which are set out below.

Individuals to be competent	All individuals introducing, promoting and distributing products must attain and maintain the skills, knowledge and expertise to perform their role competently.
Training & Competence	All individuals introducing, arranging, promoting or distributing products must undertake regular and relevant training & competence activity.
Oversight, monitoring and assessment	All individuals introducing, arranging, promoting and distributing products must be effectively supported, monitored and assessed.

Competence means having the skills, knowledge and expertise needed to discharge the responsibilities of an individual's role. This includes achieving a good standard of ethical behavior.

How do we achieve these principles?

Smart ID Training

Post Office have an 'on-boarding' process which ensures that anyone joining the business is provided with training. As part of Smart ID there is a suite of training that needs to be completed before gaining access to Horizon that includes, Anti Money Laundering, Data Protection and Anti Bribery and Corruption.

There are also two modules/tests one on Financial Services and one on Insurance Distribution Requirements that need to be completed and passed prior to colleagues undertaking financial services and/or insurance sales. These key

POL00423464

modules train and test what the regulatory requirements are, test how to undertake financial services introductory journeys compliantly and how not to advise customers.

The regulatory training is backed up with additional product training. These include distance learning packs which provide basic product information and some conversation ideas. Whilst initial training is provided, there is no structured approach to ongoing training particularly in Agency branches where the Agents are responsible for training their staff. Generally, a theme from mystery shopping is counter colleagues having little confidence or time to talk to customers about FS products. But we also must recognise here the competing priorities a Postmaster will have on their time as they are likely to be running a retail business of which the Post Office is a part.

A more in-depth initial and ongoing training programme is in place for Customer Relationship Managers (CRMs) in the Agency network. These have a more in-depth introductory journey with customers. CRMs are supported by a Training & Competence Framework managed by Area Managers and Regional Managers in the Network Field Team.

2019 Internal Audit Review of T&C

An Internal Audit review completed in June 2019 assessed the design and operating effectiveness of POL's training and oversight arrangements to ensure that colleagues who introduce and sell financial products and services within the branch network are appropriately trained and competent to support the product range made available to consumers.

The review concluded POL maintains governance mechanisms to align its training obligations and objectives with those of its Principals. Governance committees are properly set up and operate effectively, providing forums for approval, challenge and escalation of FS training and related matters.

Internal Audit rated this report '**Satisfactory**' as they found generally appropriate design and effective operation of the key controls tested with only minor control weaknesses or process inefficiencies identified

11

Monitoring

POL Conduct Compliance monitors the sale of financial service products using various methods:

- Quality of sales scorecard, which contains three streams:
    - Watch List – The purpose of the data is to highlight spikes in sales where an increase of 200% or above of their average sales over the preceding 12 months has been identified. This could suggest non-compliant or aggressive sales techniques.

      -Mystery shopping tests whether customers have been put under pressure to complete sales. In the previous financial year these

POL00423464

results have found between 92% and 99% of mystery shops did not record any such pressure.

- A file of significant complaints is received from Bank of Ireland UK and Post Office Insurance (POI). These are complaints relating to the sale of financial products and will indicate the nature of the complaint and if compensation was paid to the customer.

  -Both BoI and PoI receive a very low level of complaints related to the introduction/sale of FS products in branch. In July 2019 POI reported 0.02% of branch sales led to a complaint and for BoI the average for the last 6 months was 0.40% these are within the Principals' stated risk tolerance

- Life Insurance policies are monitored to identify those cancelled up to 30 days after the policy is sold. This is the period when the majority of policies are likely to be cancelled.

  -POI reported both over 50s and Life Insurance cancellations were within risk tolerance at the end of July 2019

- Life Insurance MI is also scrutinised separately on a monthly basis to identify multiple sales to one customer and any other unusual trends.

- Mystery shopping
  - Branch mystery shopping is completed for Savings, Over 50s and Travel Insurance. Branches are shopped if they sell the product and assessed against criteria agreed with the relevant principals, these include key sales process areas that provide assurance that Post Office is meeting its regulatory obligations. Results are issued on a monthly basis to the Network Field Teams to address gaps with the relevant branches, results reported monthly.

  - Video mystery shopping is used for Customer Relationship Managers (CRM) who use Tablets to introduce and sell financial service products. Each CRM is shopped at least 3 times a year this would increase if issues are identified.

- Ad-hoc MI such as specific complaints regarding a product sold in a branch or a process that did not adhere to agreed procedures. Examples:
  - A colleague in a branch trying to use their own debit card to pay for a customer's home insurance policy.
  - Recording a customer interest in a product through the customer referral journey which the customer has not agreed to.

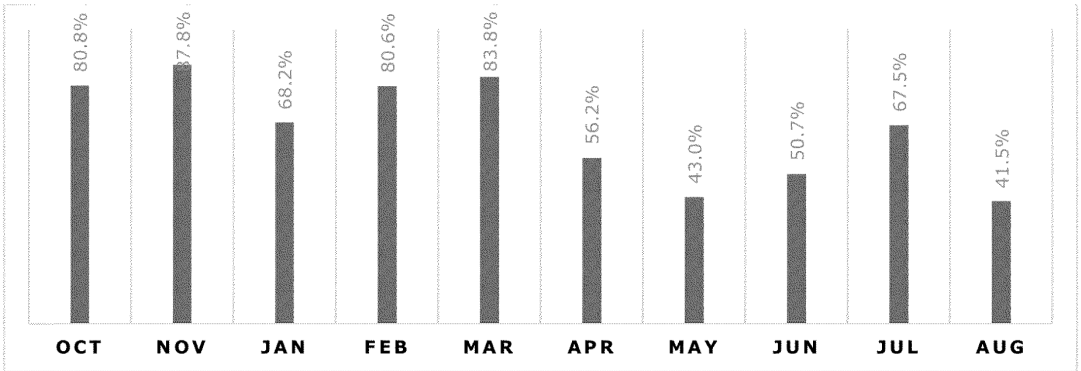
Current risks and issues identified by mystery shopping

Travel Insurance

There are a number of key parts of the sales process which are checked, the primary one is around checking the customers' medical status before providing a quote or completing a sale. This was a key change introduced following the

POL00423464

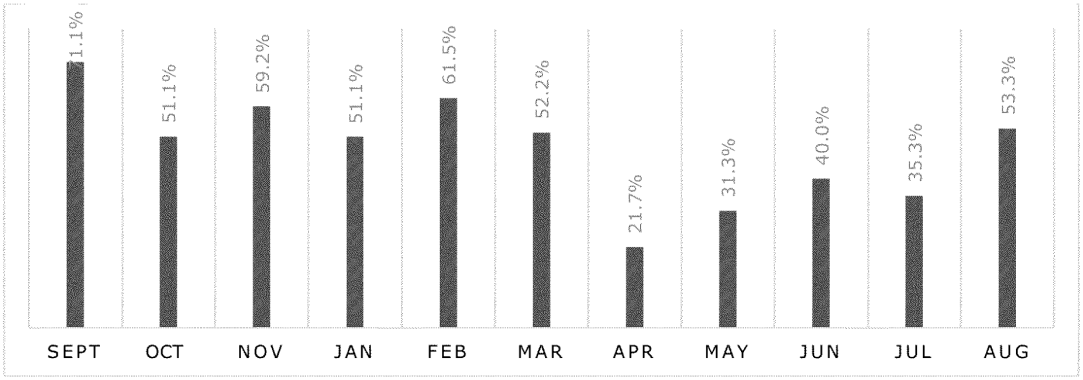
Insurance Distribution Directive (IDD) which became live in October 2018. Conformance for this area is averaging at 66% against a target of 90% in the period October 2018 – August 2019. This is of key concern as a customer who has not fully disclosed medical conditions could be under insured.



Immediate action was taken by POL Conduct Compliance by working with L&D to create a Travel Insurance training pack. This was distributed to the network to coincide with the Summer Travel Campaign. The training included a reminder of the sales process with clarity on each part of the process, why it was important and useful conversation ideas. Further training is being built for Q3 as a refresher on IDD, and will include its purpose and benefits to customers. The training will again include a reminder of the correct sales process for both Travel Insurance and Over 50s.

Over 50s Life Insurance

When introducing Life Insurance to customers, colleagues are expected to inform customers about the range of products. Customers should be able to make an informed decision about the product that would best suit their needs. Mystery shopping is showing that colleagues are showing a preference to Over 50s thereby increasing a risk of customers purchasing a policy which may not meet their needs. Conformance for this area has dipped, average for the period September 2018 – August 2019 is 48% against a target of 90%.

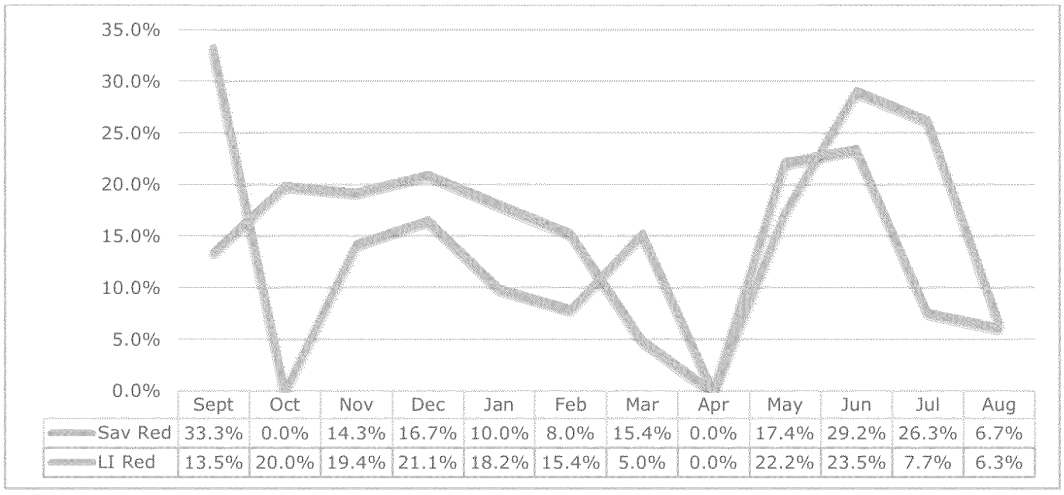


POL00423464

CRM current risks

Customer Relationship Managers (CRM) use Tablets to introduce and sell products to customers. They are video mystery shopped on Savings and Life Insurance (Easy life and Over 50s). The tolerance agreed with both Principals is no more than 10% reds. The monitoring data below demonstrates that we have struggled to meet this target consistently. The average in the period September 2018 – August 2019 is 14.5% for both products

Personal Loans was added to the Tablet in February 2019, this allowed the CRM to introduce the product, provide an indicative quote and complete a Fast Checker to allow the customer to see the likelihood of being accepted for the loan at application. As a result of a high level of Personal Loans mystery shop fails, POL Compliance agreed with BOI to 'switch off' the Personal Loans functionality until training is revised and CRMs re-trained. The changes to the screens are currently being built.



	Sept	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug
Sav Red	33.3%	0.0%	14.3%	16.7%	10.0%	8.0%	15.4%	0.0%	17.4%	29.2%	26.3%	6.7%
LI Red	13.5%	20.0%	19.4%	21.1%	18.2%	15.4%	5.0%	0.0%	22.2%	23.5%	7.7%	6.3%

11

CRM ACTIONS IN PLACE

Root cause analysis has pointed at the need for some better support for CRMs in following the compliant sales process.

To bolster support for CRMs a new support structure for CRMs has been agreed and went live in August 2019. Four dedicated Area Managers who are very enthusiastic supporters of this opportunity have been given specific training and support from POL Compliance and the Training Team. The training was designed to enable them to provide better quality support to the CRM team helping to build skills and confidence for engaging conversations and improved quality sales by helping customers to make better informed decisions.

Although early days, since going live with the new structure we have seen a dramatic reduction in the volume of Red VMS results (2 Reds out of 24 shops –

POL00423464

8.3% since the new structure went live in mid-August). If performance continues at the current levels, we could be green on a 3-month basis for both Life Insurance and Savings by the end of October.

OTHER ACTIONS IN PLACE

Travel Insurance Mystery shops have highlighted a need for a focus in this area and robust use of medical laminates, but correct knowledge is also key to compliance and risk mitigation.

We will take the following actions:

- Remove the TI product from branches that are generating high risk by not conforming to the sales process. Area Managers will work with these branches to bring them to compliance, allowing us to enable them to sell TI again.
- Force distribute the medical laminate, one per counter position to all branches selling TI, with clear instructions for its use.
- Our Area Managers will prioritise visits to high volume branches prior to peak trading periods, ensuring compliant readiness for high risk trading times
- Map the journeys customers currently take, identify pain points and areas of increased risk of non-compliance and reduce the risk in the new journey design. Informing the new TI product journey, due to be launched in Q4
- Refresh the Distance Learning Pack and send out to all TI branches, followed up with contact from Area Managers to ensure branches are actively using the DLP to refresh their knowledge
- Interrogate our H1 voice of customer data to uncover any trends across TI transactions.
- In real time, when customers highlight Irritation with TI through our customer feedback system, we will make appropriate interventions within 48 hours to investigate.

While many of our defined actions are immediate, others will embed robustly over time. We expect correct use of the medical laminate with every customer and mobilising this to every counter colleague, in every TI branch will follow a longer flight path and will become part of BAU operation. We anticipate an improvement over the second half of the year, leading to a sustained and continued improvement as we move into the new financial year.

Actions aimed at Counter Colleagues specifically:

- Using mystery shop results to improve training materials in particular where results show low levels of confidence, knowledge and skills. For example:
  - re-training of the Travel Insurance Sales process;
  - discussions with POI Compliance/product teams to help colleagues introduce the range of life insurance products by having one leaflet showing the range of products

POL00423464

- Root cause analysis - talking to branch colleagues to understand why sales processes are not being followed to identify areas for improvement to systems and also training;
- Monthly communication to the Head of Network on latest results and trends to allow for focussed actions to be taken, for example, mystery shop results and trends, reminders of upcoming changes to products and processes;
- A collaborative working group - Sales Quality Improvement Group - has been set up between Post Office Insurance and Post Office. The group consists of product managers, compliance teams from POI and POL, training and representatives from the Network field teams. The group's purpose is to work together to understand areas of weakness and agree actions to improve the quality of POI sales.

Additional actions:

- Capability Training Events – The retail network teams are holding various capability events for both CRM's and bigger Mains branches throughout September/October. These events will be run by the FSCM's and will focus on in-depth product knowledge around our savings ranges, and a separate session will focus on growing the capability of our CRM's paying attention to the latest VMS results and action planning accordingly.
- Quarterly Capability Events – Each region will be running some smaller events within certain defined geographical areas to grow the capability of branches where we feel a risk has been or could be identified. Focus will be across all FS products where the agenda will be shaped according to latest results/trends.
- Joint team meetings across the region between the Field Team AM's and the FSCM/BOI business control teams to continue to grow not just their own capability but to action plan against results where required. Refresh with Area Managers using the Branch Information tool, along with regular complaints data to coach behaviours in all branches where highlighted.
- Extend voice of customer accounts to all teams operating in the field so that they can see customer feedback before interacting with a branch.

Jonathan Hill
Compliance Director

Amanda Jones Retail Director **September 2019**

POL00423464

Monitoring of Multiple Retail Partners

Author: Karl Oliver Sponsor: Amanda Jones Meeting date: 23 September 2019

Executive Summary

Context

This paper provides an update on the monitoring of financial stability and Post Office relationships for key multiple retail partners and updates on proposed development/next steps.

Questions this paper addresses

- How do we monitor the financial stability of our key multiple partners?
- How do we monitor the relationship between the Post Office and key multiple partners?
- How do we further develop our ability to identify risk?
- What are the current partner risks?
- What are we doing to address the risks of partner failure/resignation?
- What are the next steps?

Conclusion

- The Partner Resilience tracker is new has been developed to identify signs of distress within partner finances, tracking financial KPIs aligned with BEIS tracking of major contractors and internal KPIs around partner engagement.
- Target financial ratios are impacted by industry and size of company and we are refining trigger points for each company.
- Extended trend and expansion of tracked partners beyond the initial set will identify comparators and build accuracy.
- Following a trigger a deeper review of partner performance will be completed, with possible outcomes being a shortened review cycle, partner engagement or formal contingency planning.
- Partner/PO Relationship is monitored using new openings, resignations, PO P&L and feedback as indicators of engagement
- Recent Post Office resignation activity and half-year performance has triggered McColls to 'Amber' status (following a more detailed review).
- The journey following the collapse of 'Bargain Booze' is well documented. The document is focused on administrator engagement, with an expected outcome of continuing to trade on-site and does not cover all eventualities.
- Further work is required to strengthen mitigation around both onsite and offsite solutions.
- Next steps will develop the tracker and contingency plans for partner failure.

Input Sought

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

12

POL00423464

The Report

How do we monitor the financial stability of our key multiple partners?

1. Following engagement with Risk, BEIS, Finance and the Commercial Partnership team the tracker was established in P1, to formally review finances and account activity for the 5 largest partners by volume of branches (McColls, The Co-operative Group, Tesco/One Stop, WH Smith and AF Blakemore). This Commercial Partner team and Finance business partner are responsible for updating the tracker each period for review by Retail & Finance Director. The P4 summary is included as Appendix (1).

2. The financial measures where appropriate have mirrored those tracked by BEIS and are reviewed by period looking for any indication of distress. External distress signals would include –
    - Profit warning
    - Cash constrained – low liquidity headroom
    - Prospective covenant breaches
    - Poor financial ratios particularly gearing, operating margin, ROI/ROA
    - Credit status downgrade
    - Share price underperformance
    - Failed refinancing
    - New management team

3. We currently track share price and trend, Experian ratings, key ratios (Net Debt vs EBITDA, Total Debt vs Equity and Earnings / Interest payments) and formal announcements from the partner with the aim of creating a Financial RAG rating for each partner.

4. Tracking of industry media & social feeds and insight gained from relationships is included under internal measures, notes and/or fed back through weekly Commercial Partner updates to Retail Director.

5. Ratios are impacted by both industry and size of company and further work is required to establish 'norms' and trigger points. Expanding the list of partners tracked will help by establishing comparators and length of trend-line will further refine trigger levels.

6. Following a trigger a deeper review of partner performance will be completed, with possible outcomes being a shortened review cycle, partner engagement or formal contingency planning. Escalation, whether through review cycle or

POL00423464

incident, would be to Retail and Finance Director. The format for a deeper financial review has been established in conjunction with Adeola Oke (Strategy Director) with an example within Appendix (2).

How do we monitor the relationship between the Post Office and key multiple partners?

7. The tracker incorporates a number of Internal / Relationship indicators, which whilst 'softer' are equally key in tracking risk as our most financially robust partners continue to review the value of their Post Office estate. The current set of Internal indicators are –

- IRRELEVANT

8. Working with partner groups, collective Co-ops under their Federal Retail Trading Societies (FRTS) banner and with 'SPAR UK' increasingly bringing the 5 SPAR Regional Distribution Centres (RDCs) together, formalises the feedback mechanism. This formal mechanism for the Coop has helped us to focus in on operational efficiencies across the c.500 coop sites to identify significant savings.

9. A schedule of top-2-top meetings at individual partner level and less formal engagement picked up through industry and representative events (ACS, IGD etc.) completes the 'Internal feedback' mechanisms.

How do we further develop our ability to identify risk?

10. Steps to further develop the tracker include –
    - Expanding the number of partners tracked to include
        i. Partners with 50-100 PO estate
        ii. Regionally dominant partners
    - Reviewing the measures and alternatives with Risk/Finance/BEIS group
    - Establishing trigger levels by partner
    - Individual partner trend tracking view
    - Review following an incident – "should we have seen it coming?"

11. We are documenting the escalation process triggered by a change of status on the tracker. This includes mapping the process flow, the 'deeper' review format (if triggered by a finance lever) and appropriate response at each

12

POL00423464

level/outcome to improve quality and consistency of response. Flow draft included in Appendix (3).

12. Further work is required to map out all possible outcomes of a partner entering administration and risk associated with each. This will allow POL to better develop pre & post administration plans for both partner and administrator engagement.

What are the current partner risks? (example of process)

13. McColls status is IRRELEVANT with the remaining 4 partners on IRRELEVANT. In this instance the response to IRRELEVANT has resulted in stepping up contingency planning against further reduction in size of estate, partner engagement seeking commercials from resignation sites and review schedule (asked for lease break dates/estate make-up/etc).

14. A review was triggered following the release of their H1 accounts, coupled with their recent estate activity (resignation from 17 McColls POs and 20 McColls PO sites up for sale).

15. Summary of McColls review (12/8/2019)

IRRELEVANT

12

16. Their financial results triggered a short spike in trading but has not seen any significant shift in share price. With trade and financial commentary pointing towards McColls 'doing the right things' under tough trading conditions.

17. McColls remain positively engaged with POL and have opened c.40 new locations in the last 12 months. The resignations follow store reviews which

POL00423464

have been triggered by lease breaks and all appropriate notice periods will be observed.

What are we doing to address the risks of partner failure/resignation?

18. Wider contingency planning against a partner failure has commenced with work to document existing processes for onsite and offsite outcomes. With c.450 new sites found each year there is expert knowledge within the change teams to identify temporary and offsite solutions which needs to be formally documented. External expertise has been sought to assist with mapping administration outcomes/likelihoods, POL responses to each scenario and subsequent validation. This will be focused on achieving continued trading and then onsite solutions through the administrators.

19 **IRRELEVANT**

20. An initial workshop to identify alternative 'replacement' solutions has taken place. The workshop identified a number of changes that would assist in the process (advanced mapping of estate including point 19 above) and some more 'left-field' ideas that will need to be validated.

21. The expected output of this work will be a validated scenario and response flow for partner failure to include engagement plans for partner and administrator and operational plan for any replacement activity.

What are the next steps?

22. Further development of the tracker to include more partners, establish trigger points against each measure and improved individual partner view – for inclusion from P6

12

We are continuing the work on the IRRELEVANT partner failure plan with an expected completion date of 4th October 2019, to include…

23. Fully documented partner failure scenarios and likelihoods of outcomes.
24. Built and validate POL responses against each partner outcome
25. Capture existing Onsite and Temporary solution process and best practise
26. Develop Operations response against large failure
27. Validate future improvement suggestions

POL00423464

Appendix 1 – Partner Resilience and Relationship Tracker (Cut from Excel)

IRRELEVANT

POL00423464

Appendix2 – Financial Review Example (Template)

Current status (likelihood and risk)

No near term liquidity pressures, however further decline in profitability may result in covenant pressures with potential lender action. Risk of further store closures due to challenging market outlook + Group focus on closing underperforming stores.

Key financial highlights

£m	1H19	FY18	1H18	FY17	1H18 -1H19 % change
Revenue	611	1,242	610	1,149	0.1%
Gross margin	*25.4%*	*25.9%*	*26.0%*	*26.8%*	*(0.6%)*
Adjusted EBITDA	13	35	16	44	(19%)
EBITDA margin	*2.1%*	*2.8%*	*2.6%*	*3.8%*	*(0.5%)*
Profit Before Tax	0.2	7.9	2.3	18	
Cash flow from Ops	13	62	38	54	(66%)
Free Cash Flow	8	14	25	11	(68%)
Cash	37	29	39	14	(5%)
Debt	127	127	152	157	
Net debt	90	99	99		(9%)
Leverage (Net debt/Adj. EBITDA)	*2.8x*	*2.8x*		*3.2x*	

1H19 liquidity headroom

Facilities (£m)	Total	Drawn	Undrawn/Available	Maturity
Term loan A	87.5	82.0	5.5	Jul-21
RCF	100.0	43.0	57.0	Jul-21
Accordion	50.0	-	50.0	
Cash			37.0	
Headroom			**149.5**	

- Decline in profitability due to flat sales + cost pressures and wage inflation
- Sales in News and confectionary segments continue to decline, offsetting growth in beers/spirits/wines/tobacco
- Outlook remains challenging with further pressures attributed to the weather and Brexit
- Risk of more store closures, given forecast continued decline in sales and bleak outlook
- No near term liquidity concerns as the Group has no upcoming major debt repayments + liquidity headroom appears sufficient to fund expected cash usage in the next 12 months
- However, covenant pressures remain. Whilst the Group was able to negotiate an amendment to its facility agreement in Nov-18, its covenant headroom at 1H19 was <10%. This poses a risk as a marginal decline in EBITDA could result in significant covenant pressure

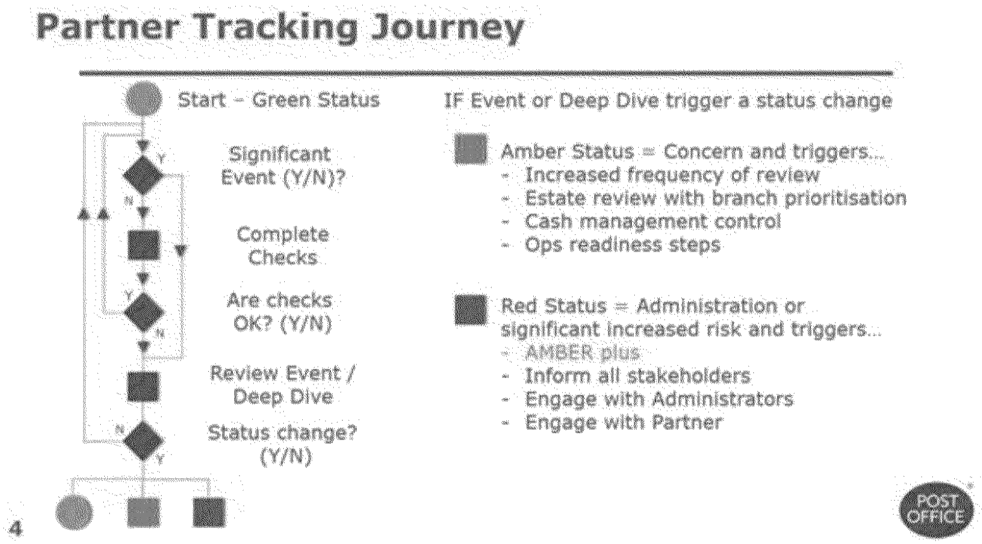
Following review status change to AMBER

POST OFFICE

6

POL00423464

Appendix 3 – Process Flow for Partner tracker triggers



POL00423464

Financial Reporting Controls Report

Author: Tom Lee, Christine Kirby Sponsor: Micheal Passmore Meeting date: 23 September 2019

Executive Summary

Context

This paper provides an update on the Financial Reporting Controls ("FRC") environment, including improvements made since the last report to the ARC in FY17/18 and details on future focus.

Questions this paper addresses

- What was the status of the FRC environment when last reported to ARC?
- What is the current status of the Financial Reporting Controls Framework ("FRCF")?
- What developments have been made to the wider FRC environment?
- What do independent sources say about the FRC environment?
- What is the future focus?

Conclusion

Since the last report to the ARC in FY17/18 there have been significant improvements made to both the primary (FRCF) and secondary (balance sheet reconciliations and associated reviews) lines of defence within the FRC environment, creating a more robust controls environment which has proved effective in FY18/19 and onwards.

The FRCF has doubled in size since the last report to the ARC in FY17/18, growing from 241 controls (March 17) to 500 controls which address 353 risks (June 19). The FRCF is substantially complete based on agreed plans in FY17/18 and focus is shifting towards enhancing the process and assessing the breadth of the FRCF. The feedback received from a recent Internal Audit ("IA") review was in line with expectations, being that the underlying FRCF is operating appropriately and, to continue to develop, we should procure a more advanced software package. This is currently being investigated.

The balance sheet reconciliation ("BS Rec[s]") templates have been redesigned in FY18/19, with gradual rollout and training for users. Additionally the balance sheet review process ("FD BS Review") has been redefined, with the focus now being on evidence-based assessment, utilising the BS Recs. These developments consolidate the processes into one; creating efficiencies in the business, placing greater onus on balance owners and ensuring transparency in business processes. The future focus is on consolidation – continuing to drive high quality balance sheet reconciliations and establishing a review process that works for all parties involved. Initial feedback from external audit is positive; they were able to use the reconciliations to assist their audit testing and they had no recommendations relating to these areas. Additionally the internal audit review of the period end process highlighted no issues in this area. Future focus is on enhancing these processes and firmly establishing them across the business.

Input Sought

The ARC is asked to note the progress made and comment on priorities.

POL00423464

The Report

What was the status of the FRC environment when last reported to ARC?

1. The last report to the ARC, which focused on the FRCF, was in FY17/18. At that time there were 241 controls within the FRCF, split across 12 processes.

2. Of these controls, 209 were live for self-assessment, with 168 being self-assessed in the period. There were 18 in remediation and the remaining controls were either in the testing phase and due to be issued for self-assessment or not submitted. See appendix 1 for a snapshot of the FRCF as at FY17/18.

3. Planned development of the FRCF at that time focused on adding in a number of processes, including: master data; agent debt; transaction corrections and agent remuneration. See point 10 onwards for a progress update on developments.

4. The FRCF is deemed the first line of defence in the FRC environment, given it prevents and detects issues at source. However, second line of defence controls existed, with the primary items being BS Recs and the FD BS Review process. Details on the development of these areas can be seen from point 12 onwards.

What is the current status of the FRCF?

5. As at the end of June 2019, there were 500 controls within the FRCF, split across 26 processes, which addressed 353 individual risks. This is a 107% increase in documented controls since FY17/18. Of these controls, 472 were live and ready to be issued for self-assessment, with the remainder being control gaps (control designed and documented but not in operation). See appendix 2 for a snapshot of the current status of the FRCF.

6. Of those issued for self-assessment in June 2019, 91% were reported as operating effectively. For the remaining 9% issued in the month, half were not submitted and half were submitted but noted as not operating. All negative responses are followed up by the Central Finance team ("CF") and amendments are made to the FRCF as required e.g. change of ownership, update of control wording, education of system usage for control owner, etc. Overall the return rates, when combined with the reasons for issues arising, are not deemed to pose a risk to assurance levels. Nonetheless, focus is being placed on reducing levels of non-returns.

7. Of the 28 control gaps (FY17/18: 18), only 2 were noted as high risk. All gaps currently identified within the FRCF have mitigating controls in place and monthly monitoring of gaps is performed. The two high risk gaps relate to:

	Risk:	Issue causing the GAP:
1	Inappropriate or unauthorised user access changes can be made in the cash management system (CWC).	The CWC system does not have user access reporting functionality.
2	Cash centre transactions are not fully reflected within the finance software (CFS).	Issues identified within the CWC to CFS interface, preventing full transfer of transactions.

POL00423464

8. These high risk gaps are mitigated via 1) manual monitoring of changes made to user access within the CWC cash management system and bi-annual user access review, and 2) weekly manual reconciliation on the CWC to CFS interface, with all reconciling items identified and investigated. Note the reconciliation issues are due to be resolved by Dec 2019, with the volume of reconciling items having reduced from c.30,000 as at FY18/19 yearend to c. 3,000 as at time of writing this report.

9. The increase in volume of controls is due to both substantial completion of the development plan as agreed in FY17/18 and the redesign of a significant number of controls following changes in processes and systems.

10. The most significant processes added to the FRCF since FY17/18 include: agent remuneration (55 controls); transaction corrections (48 controls); agent accounting (17 controls); and master data (32 controls).

11. Controls which have been redesigned following changes in systems and processes include:
    - Payroll – implementation of SuccessFactors, resulting in 42 additional controls.
    - Integrated Settlement and Billing ("ISB") – implementation of new system functionality requiring the design of a set of integrated controls.
    - Bank and cash management – split out and rework to better reflect the operational structure of the business and factor in the change in cash management system to CWC.

What developments have been made to the wider FRC environment?

12. Accounting errors identified in FY17/18 highlighted the need to strengthen the second line of defence within the FRC environment.

13. The primary tools in this area are the BS Recs and the associated FD BS Review process. A strong BS Rec should provide enough detail to allow the user to understand the nature & drivers of the balance whilst containing supporting evidence so as to allow the balance to be interrogated.

14. Over the past 12 months the BS Recs have been transformed in order to better capture these fundamental aspects. Gradual rollout of the new template across the business was accompanied by user training. These training sessions underlined the importance of high quality BS Recs and clearly defined the roles and responsibilities of both preparers and reviewers. In addition, CF has designed a formal central review process to monitor and enhance quality of BS Recs. All this has contributed to a renewed focus on balance sheet accuracy and accountability.

15. Working in tandem with the new template rollout, the FD BS Review, which has been in operation for a number of years, has been redesigned. Historically this process was very manual and centred on discursive assessments. The redesigned approach extracts data and support from the new BS Recs to generate a review file for each business unit. This facilitates timely review and challenge by both CF and divisional finance teams, and reinforces divisional FD ownership over the balance sheet. The frequency of

13

POL00423464

the reviews has been altered to drive more in depth balance sheet analysis by responsible parties, the fundamental premise being that a balance must be supported by auditable evidence which will be challenged periodically.

16. Although significant improvements have been made, these processes are still being developed to ensure appropriate assurance is achieved. Some areas of the business are yet to be rolled onto the new templates e.g. Supply Chain; however, plans are in place to complete this in FY19/20.

17. Looking beyond general process improvements, where issues have arisen across the business that impact the key concerns of the FRC, focus has been placed on addressing these in both the short and longer term. A key focus area has been the over reliance on third party data for revenue recognition, where concerns arose following the Telecoms error identified in FY17/18.

18. During FY18/19 a full review was performed on the processes and controls adopted by these third parties in order to establish whether reliance can be placed on the information provided. The work was carried out by both CF and Grant Thornton. Across the 13 suppliers assessed, there were no significant findings noted, beyond those established in FY17/18, with all minor findings being reported to responsible parties to act on.

19. The frequency and depth of these reviews is being discussed internally, to ensure adequate assurance is achieved. Internal processes and controls around third party data are currently being assessed and developed; we expect the frequency and depth of reviews to thus reduce going forward.

20. The results of the control self-assessment ("CSA") were reported to the CFOO (now reported to Group FD) on a monthly basis. Since FY18/19 the reporting has been extended beyond the FRCF to include all aspects of the FRC environment, i.e. both the CSA results and the status of the second line of defence controls, along with any other pertinent items as at that time.

21. Additionally, since FY17/18, annual testing of the FRCF has been completed internally by CF to assess the design and operational effectiveness of the FRCF. The results of which are reported to the Group FD.

What do independent sources say about the FRC environment?

22. Internal Audit conducted a review over the FRCF in Q4 FY18/19. The result of the audit was "requires improvement". The findings were in line with our expectations, being no issues with quality or suitability of the processes and controls. Of the 7 findings identified, 3 related to process formalisation/clarification (now complete) and 4 related to system limitations, beyond the scope of the FRCF.

13

23. Internal Audit also performed a review over the financial month end close process which included, but was not limited to, BS Recs and the FD BS Review. The result of this audit was "satisfactory" with no findings in relation to these aspects.

POL00423464

24. The external audit identified minimal management letter points, none of which concerned the FRCF or other FRC related processes discussed in this report. The audit findings were principally related to differences of opinion on judgemental areas or the classification of balance sheet items, neither of which are indicators of issues within the FRC environment. Furthermore, FY18/19 is the first year an external auditor has placed reliance on BS Recs to support their audit, evidencing the enhanced quality of this area.

What is the future focus?

25. The FRCF focuses on Financial Reporting Controls, therefore the next phase is to identify additional areas to be captured in order to develop the framework into a full Financial Controls Framework, thus mitigating wider financial risks.

26. Finalisation of known development area's such as master data, cash forecasting and ISB which are all substantially complete but require re-review.

27. Looking beyond completeness of processes within the framework, the quality and effectiveness of controls along with increasing ownership within the organisation are a future focus. System limitations prevent accessible ownership beyond the control owner level, to that of process owner or sponsor, however a new system should allow development in this area.

28. In order to achieve this, whilst addressing the system concerns that we and IA have noted, the following are currently being performed / are planned for the near future:
    - End to end risk and process reviews for all areas within the FRCF;
    - Process split out within the FRCF to better reflect ownership structures; and
    - Identification of a replacement self-assessment tool, to allow:
        i. Enhanced reporting, including historic and comparative reporting
        ii. Risk focused perspective, including dashboards and reporting
        iii. Workflow for control owners, process owners and CF
        iv. Linkage between risks, controls and process mapping
        v. Gap & remediation management and escalation
        vi. Self-service system administration to allow quicker response rates

29. Continual development of the BS Recs and associated FD BS Review process in order to get the right balance between independent central review and ownership by divisional finance teams. In order to assist with this, we are investigating the potential of acquiring a balance sheet reporting tool which would aide workflow, reporting and risk identification.

30. Being reactive and proactive in regards to wider changes within the business. A number of areas being reviewed presently are:
    - Payzone - high level review was performed after acquisition. In depth review is scheduled to be performed off the back of the IA visit in September 19.
    - Source to Settle project – working with the project on control development.
    - Project approval – review of the process and controls to ensure the right level of CF involvement at the early stages.

POL00423464

Appendix 1 - March 2017 Control Self-Assessment Reporting

Total Controls	Control Gaps					Control Owners		March CSA Results				
Process	Total Controls	Control Gaps	H/M/L Impact of H	M	L	Owner Assigned	No owner assigned	Controls operated effectively	No self assessment submitted	Not operated due to agreed frequency	Self assessment submitted but control not operated	Controls to be set to live
Bank & Cash Management	33	2	0	2	0	32	1	28	0	2	0	0
Bill To Cash	17	3	0	2	1	17	0	12	0	2	0	0
Control Environment	21	1	0	1	0	21	0	8	0	1	0	11
Fixed Assets	18	3	0	0	3	18	0	14	0	1	0	0
Payroll	34	1	0	1	0	34	0	29	0	4	0	0
Procure To Pay	24	1	0	1	0	24	0	12	1	10	0	0
Project Accounting	9	2	0	2	0	9	0	3	2	2	0	0
Record To Report	38	3	0	3	0	38	0	30	0	5	0	0
Settlement Process	14	0	0	0	0	12	2	12	0	0	0	0
Stock	7	2	0	1	1	7	0	5	0	0	0	0
Tax	16	0	0	0	0	16	0	7	0	9	0	0
Treasury	10	0	0	0	0	10	0	8	0	2	0	0
	241	**18**	**0**	**13**	**5**	**238**	**3**	**168**	**3**	**38**	**0**	**11**

Note – The 241 controls in the period are made up of 18 gaps, 168 controls operated effectively, 3 controls not submitted, 38 controls not operated due to frequency and 11 controls yet to be set live.

13

POL00423464

Appendix 2 – June 2019 Control Self-Assessment Reporting

Controls		Control Gaps				Control Owners		June 2019 CSA Results (submitted July 2019)				
Process	Total controls	Control gaps	H/M/L Impact of GAPS H	M	L	Owner Assigned	No owner assigned	Controls operated effectively	Self-assessment submitted but control not operated	Controls with long-term remediations	No self assessment submitted	Controls not included due to frequency
Agent Accounting	16	0	0	0	0	16	0	10	0	0	1	5
Agent Remuneration	55	2	0	1	1	55	0	44	2	2	2	5
Agent Remuneration Calendar	4	0	0	0	0	4	0	3	0	0	1	0
Bank & Cash Management	51	4	0	2	2	51	0	28	2	4	0	17
Bill To Cash	22	1	0	0	1	22	0	14	4	1	3	0
Cash Centre - Finance and Master Data	15	4	1	2	1	15	0	6	0	4	0	5
Cash Centre - Supply Chain	16	1	1	0	0	16	0	9	0	1	0	6
Control Environment	32	3	0	0	3	32	0	23	2	3	1	3
Fixed Assets	19	0	0	0	0	19	0	10	0	0	0	9
HMRC Registration Process	11	0	0	0	0	11	0	11	0	0	0	0
Integrated Settlement & Billing - Billing	3	0	0	0	0	3	0	0	0	0	0	3
Integrated Settlement & Billing - Settlement	11	1	0	0	1	11	0	0	0	1	0	10
Manage open items	8	0	0	0	0	8	0	2	0	0	0	6
Master data management	28	0	0	0	0	28	0	14	2	0	5	7
Non Standard Operating Model (OSF)	5	0	0	0	0	5	0	4	0	0	0	1
Payroll	29	2	0	1	1	29	0	25	0	2	0	2
Procure To Pay	28	0	0	0	0	28	0	28	0	0	0	0
Profitability (COPA)	7	0	0	0	0	7	0	0	0	0	0	7
Project Accounting	10	3	0	1	2	10	0	7	0	3	0	0
Record To Report	40	2	0	0	2	40	0	23	2	2	2	11
Settlement Process	8	0	0	0	0	8	0	5	1	0	0	2
Stock	13	5	0	5	0	13	0	4	0	5	2	2
Tax	17	0	0	0	0	17	0	13	0	0	1	3
Transaction corrections #1	25	0	0	0	0	25	0	25	0	0	0	0
Transaction corrections #2	19	0	0	0	0	19	0	19	0	0	0	0
Treasury	8	0	0	0	0	8	0	7	0	0	0	1
	500	**28**	**2**	**12**	**14**	**500**	**0**	**334**	**15**	**28**	**18**	**105**

Note – control self-assessments are submitted retrospectively and subsequently reported on. As such the June results, submitted in July, are the most recent results which have been reported to the Group Finance Director at the time of submitting this report.

Explanation of key columns:

- Control gaps – a risk has been identified and control has been designed but is not yet in operation. Mitigating controls are in place.
- Controls operated effectively – controls which have been self-assessed in the period as operating as per the control wording.
- Self-assessment submitted but control not operated – controls which did not operate effectively in the period. The system prompts the control owner to create a remediation plan if they select that their control is not operating and these are followed up by CF.
- Controls with long term remediations – controls which are not operating effectively and there is no short term solution. These controls are classes as 'gaps' and mitigating controls are put in place.
- No self-assessment submitted – controls where the owner has not completed the control self-assessment in the given period. These are followed up by CF.
- Controls not included due to frequency – controls which are not operated on a monthly basis (i.e. annual, bi-annual and quarterly controls) and were not expected to be operated in the period being reported on.

13

POL00423464

The Provision of External Auditor Consulting Services

Author: Micheal Passmore Sponsor: Al Cameron Date: 23 September 2019

Executive Summary

Context

POL is currently refreshing it's management consulting panel of suppliers using the CCS Framework RM 3745, which will see approximately 20 suppliers appointed. This will mean that upto 20 potential companies may bid to provide consulting type services for specific work into POL, of which PwC is one.

As our former internal auditor, they have not picked up any significant consultancy work from POL in recent years. They have now been invited to join the panel and bid, however they have sought clarity on what permissible non-audit services would be considered wholly acceptable given their new position as external auditors. This paper covers the general non-audit services any POL appointed external auditor should be excluded from bidding for and providing services on.

Questions addressed in this report

1. What services are included in the management consulting services RFP?
2. What non-audit services should the external auditor be excluded from bidding for and providing services on?
3. Should any fee caps be imposed on non-audit fees?

Conclusions

It is clear that the external auditor cannot provide management consulting services for all types of work; the list of services we believe should be excluded are defined in section 5. This restriction should not deter them from providing services to areas of work where there is no conflict of interest around their current provision of external audit services, which would otherwise impair their judgement, alignments and interdependence (ie any other service which is not defined in section 5).

Given that the external auditor isn't able to provide all the management consulting services that POL will require, it has been considered if they should be excluded from being selected onto the management consulting supplier panel. It is important for POL to encourage healthy competition and value for money services, and as such, it is better to include the external auditor, with a restrictive list of services, than to exclude.

We have considered if POL should impose a fee cap (the percentage of non-audit fees to audit fees) on the external auditor, as required in listed companies. This approach would probably preclude the external auditor from bidding due to the value of additional

POL00423464

services being capped around £400k pa. As an alternative approach to fee capping, we would report annually on the services provided to ARC, and would email the Chair of ARC as they start to bid each time, in case there are concerns we haven't thought of.

Input Sought

The ARC is requested to agree the list of excluded non-audit services is appropriate and complete as defined in section 5.

The Report

What services are included in the management consulting services RFP?

1. POL's Management Consultancy requirements vary from year to year. Below are a range of assignments based on previous experience, providing a good indication of the types of assignment which might arise. These were included in the RFP document sent to potential suppliers:
   - 1.1 Cost reduction exercises
   - 1.2 Business Change Assignments
   - 1.3 Organisational Design
   - 1.4 Pensions related advice
   - 1.5 Joint ventures and strategic alliances advice
   - 1.6 Entry into markets advice.
   - 1.7 Sale of businesses advice.
   - 1.8 Telecoms related advice
   - 1.9 Foreign exchange strategy advice
   - 1.10 Supply chain/logistics consultancy
   - 1.11 Business Case Development
   - 1.12 Propositions Development
   - 1.13 Strategy Development
   - 1.14 Risk framework activity
   - 1.15 Ownership structures
   - 1.16 Change advice
   - 1.17 Agile

2. The above list is an example and not an exhaustive view; it is difficult to cover every eventuality. It is therefore easier to agree what type of work the external auditor should be excluded from bidding for and providing services on.

POL00423464

What non-audit services should the external auditor be excluded from bidding for and providing services on?

3. PwC have provided the following list of non-audit services which they wouldn't perform for other external audit clients.

4. The list has been reviewed by POL and agreed as appropriate for exclusion.
   24.

5. Non-audit services where the external auditor will not be permitted by the ARC to provide services, are suggested to be as follows;
   - 5.1 tax services relating to:
     - 5.1.1 the preparation of tax forms;
     - 5.1.2 payroll tax;
     - 5.1.3 identification of public subsidies and tax incentives unless support from the statutory auditor or the audit firm in respect of such services is required by law;
     - 5.1.4 support regarding tax inspections by tax authorities unless support from the statutory auditor or the audit firm in respect of such inspections is required by law;
     - 5.1.5 calculation of direct and indirect tax and deferred tax and;
     - 5.1.6 provision of tax advice.
   - 5.2 Services that involve playing any part in the management or decision-making of the audited entity;
   - 5.3 Bookkeeping and preparing accounting records and financial statements;
   - 5.4 Payroll services;
   - 5.5 Designing and implementing internal control or risk management procedures related to the preparation and/or control of financial information or designing and implementing financial information technology systems;
   - 5.6 Valuation services, including valuations performed in connection with actuarial services or litigation support services;
   - 5.7 Legal services, with respect to:
     - 5.7.1 the provision of general counsel;
     - 5.7.2 negotiating on behalf of the audited entity and;
     - 5.7.3 acting in an advocacy role in the resolution of litigation.
   - 5.8 Services related to the audited entity's internal audit function;
   - 5.9 Services linked to the financing, capital structure and allocation, and investment strategy of the audited entity, except providing assurance services in relation to the financial statements;
   - 5.10 human resources services, with respect to:
     - 5.10.1 management in a position to exert significant influence over the preparation of the accounting records or financial statements which are the subject of the statutory audit, where such services involve:
     - 5.10.2 searching for or seeking out candidates for such position; or
     - 5.10.3 undertaking reference checks of candidates for such positions.
   - 5.11 Structuring the organisation design; and
   - 5.12 Cost control.

6. In general, the ARC will not give approval for non-audit services to be provided by the Group's external auditors which would result in:

POL00423464

6.1 the external auditor auditing its own firm"s work;
6.2 the external auditor making management decisions for the Group;
6.3 a conflict of interest being created; or
6.4 the external auditor being put in the role of advocate for the Group.

Should any fee caps be imposed on non-audit fees?

This relates to the ratio of non-audit fees to audit fees.

Listed companies now have to have a ceiling of 70% NAF : AF (non-audit fees cannot be higher than 70% of the average of the last 3 years audit fees). Whereas there is no such cap for non-listed entities.

If POL chose to have a fee cap in line with that of listed companies (70%), it would probably mean that the external auditor would not bid, as the maximum annual spend of IRRELEVANT would rule out all but smaller pieces of consulting work and become a practical impediment to engaging them.

There is currently a PwC in-house safety-net put in place to ensure there is internal consultation to confirm their independence is not impaired/there are no conflicts of interest. This covers for non-listed companies there is a requirement for the audit partner to consult with the in-house Ethics Partner, if non-audit fees are expected to be greater than 3 times the annual audit fee.

14

POL00423464

Notes for ARC meeting Monday 25 November 2019

- Time: 16.00pm – 18.00pm, Room 1.19 Wakefield.
- Nigel Boardman (BEIS ARC Chair) will be observing the meeting.
- NEDs are due to meet Internal Audit without management present.