POL00423567

Risk and Compliance Committee Agenda

Date:	Thursday 9 May 2019	Time:	13.00 – 16.00	Location:	1.19 Wakefield

Present:	Other Attendees:	
• Alisdair Cameron (Chair) • Cathy Mayor (deputising for Debbie Smith) • Chrysanthy Pispinis (deputising for Owen Woodley) • Mo Kang (Group HR Director) • Rob Houghton (Group Chief Operating Officer)	• Veronica Branton (Head of Secretariat) • Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Jonathan Hill (Compliance Director) • David Parry (Senior Assistant Company Secretary)	• Liz Robson (items 3, 7) (Change & IT Director – Retail) • Nick Boden (item 6) (Senior Product / Travel Director) • David Meldrum (item 7) (Head of IT Security) • Tim Armit (item 8) (Business Continuity Manager) • Clare Hammond (item 9.1) (Senior Data Protection Manager)
Apologies: Debbie Smith, Owen Woodley, Mick Mitchell		

Agenda Item		Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest**	Noting	Chair	13.00 – 13.05
2.	**Minutes and Action Lists**	Approval		(5 minutes)
3.	**PCI-DSS Update (verbal)**	Noting	Liz Robson	13.05 – 13.15 (10 minutes)
4.	**Internal Audit** **4.1 Internal Audit Report**	Noting & Input *Onward submission to the ARC.*	Johann Appel	13.15 – 13.45 (30 minutes)
5.	**Risk** **5.1 Consolidated Risk Report incorporates:** • **Impact of Litigation Outcomes and associated risks (Appendix 1)** • **Executive Declarations (Appendix 2)** **5.2 Risk Management Section for Annual Report and Accounts**	Noting & Input *Onward submission to the ARC.*	Jenny Ellwood	13.45 – 14.25 (40 minutes)
6.	**Compliance** **6.1 Consolidated Compliance Report incorporates an update on fit and proper**	Noting & Input *Onward submission to the ARC.*	Jonathan Hill/Nick Boden	14.25 – 14.55 (35 minutes)
7.	**Security Strategy** **7.1 Cyber Security Update incorporating the Security Strategy Update and the Closing report on PZBP pen testing**	Noting & Input *Onward submission to the ARC.*	David Meldrum/Liz Robson	14.55 – 15.25 (30 minutes)
8.	**Business Continuity Plan** **8.1 Business Continuity Plan update including Business Continuity Management Policy for approval**	Noting & Input	Tim Armit	15.25 – 15.35 (10 minutes)

Strictly Confidential

POL00423567

Risk and Compliance Committee Agenda

9.	**Noting Papers**			
9.1	**GDPR Update** *Assessment on our level of compliance from a regulatory risk perspective and to assess whether we had a sustainable position*	Noting	Clare Hammond	15.35 – 15.45 (10 minutes)
10.	**Review of draft Audit, Risk and Compliance Committee meeting agenda** Note: The next ordinary ARC meeting will be held on 29 May 2019	Discussion	Chair	15.45 – 16.00 (15 minutes)
11.	**Any other Business** Note: The next ordinary RCC meeting will be held on 4 July 2019.	Discussion	All	

POL00423567

2

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 14 March 2019 at 11.30 am

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

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

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

2. Minutes and Action Lists

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

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

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

3. Internal Audit (IA)

3.1 Internal Audit Report (IAR)

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

POL00423567

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

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

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

A number of points were raised:

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

3.2 Draft Internal Audit Plan 2019/20

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

A number points were raised:

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

POL00423567

4. Telco

4.1 FIN11 issue and Telecoms Controls

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

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

A number of points were raised, including:

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

4.2 Text Relay

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

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

[1] Which went down to customer levels.

POL00423567

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

5. Risk

5.1 Consolidated Risk Report

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

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

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

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

5.2 Brexit Update

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

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

5.3 Back Office Transformation (BOT) – Legacy Risks

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

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

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

POL00423567

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

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

A number of points were raised, including:

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

6. Compliance

6.1 Compliance Report

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

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

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

6.2 Fit and Proper: Compliance with HMRC June 2019 Deadline

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

All agents and assistants should have been vetted at appointment but the HMRC regulations in relation to travel money transactions went beyond this. Where we could not provide evidence of compliance with

POL00423567

HMRC requirements we would "switch off" those branches[3] until we could provide the required information. Branches with the highest revenue were being targeted but we were likely to have a tail of small turnover branches. By the next RCC we could show the impact of turning off some branches. There is a separate question as to registration of branches with HMRC.

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

A number of points were raised, including that:

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

7. Annual Legal Review

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

8. GDPR Update

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

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

9. Cyber Security Update

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

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

POL00423567

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

A number of points were raised, including:

- what progress had been made with the cultural and educational programme? It was reported that communications had been issued and were continuing to be issued. There were going to be roadshows at key PO sites. Keeping the communications fresh and live and part of a "BAU" programme was discussed. Disruptive communications and approaches were being discussed at the next Information Security Committee and messaging was focussed on how security breaches impacted individuals
- whether we were deploying our best messaging resources? It was reported that we were working with the Communications Team. It was suggested that we should also be working with the Marketing Team and considering how we could use Digital Stars to support the messaging.

To do: MM/ JH

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

PCI Compliance

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

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

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

PZBP

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

POL00423567

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

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

To do: VB

10. Noting Papers

10.1 Procurement Update: Supplier Contracts out of governance

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

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

10.2 Horizon Scanning

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

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

12. Any other Business

12.1 Treasury Policy

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

12.2 Contract management

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

12.3 Meeting dates

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

POL00423567

Post Office Limited Risk and Compliance Committee Actions
Updated: 30.04.19

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
RCC Meeting 14.03.19					
6. Compliance Report					
6.2	Fit and Proper - the Programme needed to build in the decision process for switching branches off, who would be taking these decisions and the operational impacts. This process needed to be in place by the end of March 2019. Nick Boden would produce a decision matrix and ask Julie Thomas and Amanda Jones to review this. The process needed to include the PO Limited senior contract for each of the multiples so they could speak with their counterpart where data returns had not been received	Nick Boden	May 2019	To be covered in the Compliance report.	

POL00423567

Internal Audit Report

Author: Johann Appel

Meeting date: 9th May 2019

4.1

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Internal Audit activity and key outcomes. This includes details of the work completed since the last Audit, Risk and Compliance Committee (ARC) meeting in March and progress on the 2018/19 and 2019/20 Internal Audit Plans.

Questions this paper addresses

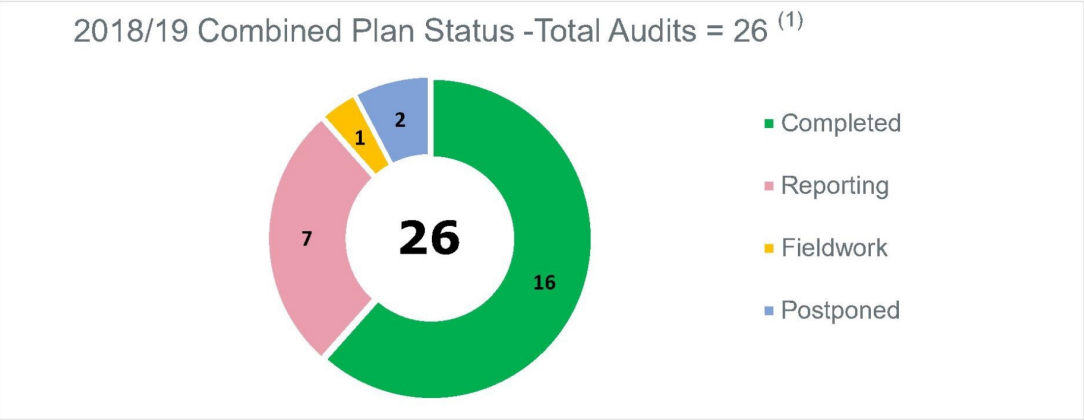
- Is the Internal Audit Plan on track? What progress has been made since the last meeting?
- Do Internal Audit have adequate resources to deliver the Audit Plan?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan (2018/19):

We have made good progress clearing the backlog of audits, following the delays experienced in 2018. We will deliver 24 of the 26 reviews on plan. The remaining two reviews are change assurance reviews, which were delayed due to the change portfolio being reprioritised. These two programmes have been included in the 2019/20 change assurance plan.

Six reviews have been finalised since the March ARC, with summaries included in paragraph 9. Current delivery progress is as follows:



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

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

POL00423567

2. Progress against plan (2019/20):
Five POL reviews and two POI reviews from the 2019/20 audit plan are being planned for delivery in Q1. More detail is provided in paragraph 10.

3. Open and Overdue Audit Actions (as at 30 April 2019):

Audit Action Status:	
Open (not yet due)	21
Overdue (<60 days)	0
Overdue (>60 days)	0
Total	21

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

4. Reporting on Control Themes:
Given the high number of reports that are still being finalised, it is not yet possible to produce meaningful mapping of audit findings against internal control themes. We will endeavour to report this information at the ARC meeting in May (or latest July) to provide coverage of the full annual cycle, with comparative results for the previous year.

5. Significant Issues:
There are no significant issues we believe the committee should be made aware of.

Input Sought

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

POL00423567

The Report

Changes to plan since March ARC meeting

6. 2018/19 Plan: As advised at the March ARC meeting, two change assurance reviews have been delayed to 2019/20 due to the reprioritisation of the change portfolio (Digitising Mails & Payment Technology Upgrade (PCI)). Both are being planned for delivery in Q1.
7. 2019/20 Plan: There were no changes made to the 2019/20 audit plan, which was approved at the March ARC meeting and is attached as appendix 2.

POI Audit Plan

8. POL Internal Audit is also responsible for delivery of the audit plan for Post Office Insurance (POI). Progress with the 2018/19 audit plan is reported at the POI ARC. Below are the current status of POI audits and summary of key findings:

Audit title and high level scope	Key findings	Status and Rating
Insurance Distribution Directive (IDD) (Readiness review). • Assessment of the Project Governance arrangements to manage the IDD regulatory change project. • Review the project documentation to assess POMS' interpretation, translation and status of solutions to become IDD compliant.	POI had been proactive in initiating the programme of IDD work to meet the implementation date of 1 October 2018. Two medium priority issues were identified: • The absence of an overarching document setting out the full scope of the project. As such, the full impact of the IDD requirements were unclear at the time of audit, which limited the programme's ability to effectively assess the amount of work needed to deliver to plan. • The lack of formalised detailed plans for each work stream that would capture and track the processes and documentation requiring changes to be made in order to comply with the IDD requirements from 1 October 2018.	Final report issued Needs Improvement
Oversight of Appointed Representatives (Assessment of governance and control design and operating effectiveness.) • Phase 1: Assess the design effectiveness of POI's controls (as Principal) over its AR relationship with POL. • Phase 2: Assess operating effective-ness of controls.	Overall a good level of oversight and governance was observed. Four medium priority issues were found: • The absence of a formalised and documented AR Framework. • A required regulatory clause was omitted from the multi principal agreement between POL and BoI. • MI required further improvement, including clarification and consistent application of risk tolerances. • The absence of a clearly articulated and documented procedure that sets out how POI performs due diligence and assesses risk in relation to its AR relationship with POL.	Phase 1 – Final report issued Needs Improvement Phase 2 – Moved to Q1 2019/20

POL00423567

Product Lifecycle - Assessment of governance and controls activities over product development, design, monitoring and review.	Fieldwork expected to be completed 6 May.	Nearing end of fieldwork
Nemesis - Programme assurance with focus on programme initiation, oversight, requirement capture and current phase delivery.	Report is being reviewed by management.	Reporting
MI - Assessment of the controls in place to ensure completeness accuracy of feeds received from key interfaces (Duck Creek, Alice-Royal London-; Junction BI Module, etc.) into the MI Platform.	Audit was delayed due to delay in the design and implementation of the new MI platform. POI ARC requested that in the interim this review be re-scoped to assess the completeness and accuracy of the feeds from key interfaced systems. Fieldwork expected to be completed 31 May.	In progress

Internal audit reviews completed

9. Since the March ARC meeting we have finalised the following six reviews:

- Client Settlements Process
- Branch Hub / Agents Portal (Change Programme)
- Network Reporting
- Cyber Security Maturity Assessment
- Digital Identity (Change Programme)
- Agent Remuneration

Our findings and observations from these reviews are summarised below:

Client Settlements (Ref. 2018/19-20)

Satisfactory

Sponsor:
Al Cameron

Audit actions:

P1	0
P2	3
P3	1
Total	4

The Client Settlements process has changed significantly as a result of the Back Office Transformation Programme. The Client Settlements team currently services 220 clients, with payments to them totalling an average of £460m per week.

We conclude that the implementation of BOT Systems went well and the controls over Client Settlements, both before and after BOT, were found to be well established and generally effective with particular emphasis on strong user access controls and segregation of duties. Although some areas for improvement have been highlighted, we have found the control environment to be acceptable and therefore we have rated this report '**Satisfactory**'.

Management Comment provided by Micheal Passmore

"I am pleased to see that we continue to maintain a strong controls environment and we will, of course, look to act on the recommended changes identified."

POL00423567

Branch Hub (Change Assurance) (Ref. 2018/19-15)

Needs Improvement

Sponsor:
Rob Houghton & Debbie Smith

Audit actions:

P1	0
P2	6
P3	4
Total	10

Branch Hub is a strategic programme set to deliver a new digital channel that enables 24/7 access to services fundamental to Agents. The programme initiated in October 2017 with key development starting from May 2018, with a scheduled Minimum Viable Product (MVP) go-live in October 2018. The programme experienced delays, re-prioritised its deliverables and deployed an 'Alpha' pilot with a more limited set functionality in November 2018.

This change assurance review adapted its focus and timeline to accommodate the re-plan. We highlight the following key observations:

- While we observed significant progress improving on the learning of previous digital deliveries, with an overall adequate governance and programme management, our review still highlighted weaknesses in the design and operating effectiveness of core process such as programme benefit assessment, risk management and requirement capture and documentation. There was an initial lack of clarity over roles and responsibilities and lack of resources in the PM/PMO space.
- The key contributor for the delay of MVP was the delays in assessing and agreeing the underlying solution architecture. The primary responsible was Fujitsu and the changes in their cloud strategy impacting the wider proposition for Post Office under Belfast Exit.
- The programme follows the Agile delivery methodology. However, the maturity over Agile is low in Post Office and this also contributed to the delays and has impaired the fast mobilisation and management of Fujitsu resources.

We have rated this report **Needs Improvement**, emphasising the ambition to drive immediate improvements as observed following the review. At January 2019 Investment Committee (IC) additional funding approval, a clearer roadmap of planned features and Agent adoption targets was submitted and the plan to address key noted deficiencies was well underway.

We have also been working closely with the SPO as some control themes noted were flagged as common to other programmes. These issues were elevated to portfolio level actions and are now part of the deliverables under Change Excellence.

Management Comment provided by Andy Garner (Product Manager for Branch Hub)

"Branch Hub Digital Delivery team agree good progress is being made in embedding agile delivery methodology. It is recognised that the low level of Fujitsu agile maturity has held up our mobilisation of features however this and delivery performance is improving. It is accepted that the controls and processes need to be tighter around e.g. benefits management and risk management."

Management Comment provided by Kevin McKay (Delivery Performance Manager, SPO)

"SPO recognise the need to drive improvements in agile adoption and use, and to provide tools and standard approaches to facilitate this. Whilst one action was already in progress and will be completed shortly, the other has been added to the backlog for PI4 which runs from April to June 2019."

POL00423567

Network Reporting (Ref. 2018/19-23)

Needs Improvement

Sponsor:
Debbie Smith

Audit actions:

P1	0
P2	3
P3	1
Total	4

Under the Funding Agreement, POL is required to fulfil two related but separate obligations around the total network numbers - proximity to a Post Office and delivery of services of general economic interest (SGEI):

1. To maintain a network of at least 11,500 branches for the duration of the Agreement.
2. To meet agreed network Access Criteria, largely relating to incremental percentages of the UK population being within prescribed distances of a Post Office.

POL received a Network Subsidy Payment of £70m in 2017/18, with £50m expected for 2018/19.

Post Office reports annually on its branch network numbers, services and accessibility to the Secretary of State, and ultimately to Parliament, as required under Provision 11 of the Postal Services Act 2011. UKGI have requested that the 2019 Network Report is approved by the POL Board prior to submission. POL Internal Audit was asked by the Board to provide assurance over the process by which this report is produced.

The audit objective was to assess the understanding of the requirement to report in the business and review the process and controls in place to ensure accuracy of the 2019 report. We also reviewed the proposed methodology change (to take effect from April 2019) and the process used to gain assurance that SGEI is delivered across the network.

The audit concluded that both the requirements and the importance of reporting accurate and consistent information are well understood by the teams that produce the report. The process to calculate the reported numbers and the report itself is established and the audit did not identify any errors. The new methodology has been run in parallel with the current. Management are satisfied that the intended process improvements will be realised from April 2019.

Deficiencies in the completeness of process documentation and audit trail retention were identified, and we have agreed actions with management to remediate these findings.

We have rated this report **Needs Improvement** as there are some process and control weaknesses that, if not addressed, may result in inaccurate reporting in future.

Management Comment provided by Tom Moran

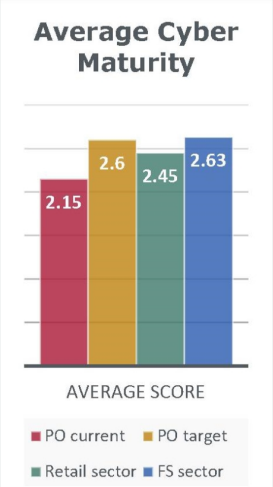
"Management are both in agreement with, and supportive of, the findings of the audit. During a time of change your recommendations to develop more robust documentation of the process is an important step and will be completed as a matter of urgency over the coming weeks. Overall, the process has been very helpful in identifying areas of improvement."

POL00423567

Cyber Security Maturity Assessment (Ref. 2018/19-22)

Not Rated

Sponsor:
Rob Houghton



Audit actions:

P1	10
P2	0
P3	0
Total	10

In December 2018, the POL Board commissioned Deloitte to assess the maturity of Post Office's Cyber Security capabilities.

The review was carried out in two phases. Phase one enabled rapid reporting of provisional maturity scores to the ARC in January 2019. Phase two involved an in-depth validation of maturity, the development of detailed recommendations for each area and allowed POL to select maturity targets through discussions with Deloitte. The review covered 34 cyber capabilities across 4 top level domains:

- Governance – how the organisation is set up to address cyber security.
- Secure - what proactive protection is in place to defend against cyber threats.
- Vigilant – how the organisation detects malicious, unknown or unauthorised activity.
- Resilient – whether the organisation can respond quickly and appropriately when a risk materialises.

Deloitte leveraged their Cyber Security Framework (CSF) and supporting tool to provide an objective and repeatable assessment of cyber maturity. Strong buy-in and support from the business, in particular the IT Security, IT Risk, Information Protection and Assurance, and Physical Security teams allowed Deloitte to quickly identify relevant information and provide a focused analysis of strengths and opportunities.

Deloitte concluded that Post Office has made significant progress over the last 12 months in developing its IT and information security capabilities. Increases in maturity scores between phases one and two of this review confirmed progress made in the first 3 months of 2019. Nevertheless, a total of 224 recommendations were identified across 34 cyber domains – these are currently being analysed to identify any maturity gaps that are not yet addressed by the IT Security Transformation Programme (ITSTP). It is encouraging that actions to address 76% of the capabilities, where a maturity shortfall was identified, are already in progress or included within the STSTP.

Implementation of the 10 overarching actions, combined with a focus on addressing high priority actions as part of the ITSTP, will allow POL to make significant progress in reaching its target maturity levels. Follow-up maturity assessments will enable the business to track progress against targets and to address changes in the cyber security landscape.

As this review was commissioned as an independent maturity assessment, it was not rated.

Management Comment provided by Mick Mitchell

"We accept the findings of this assessment. We also welcome the benchmarking and targets that have been set to judge IT Security maturity going forwards. This assessment gives a repeatable process and a clear and measurable focus for the future.

It is also reassuring that the ITSTP already has a large section of the actions needed included. However, we will review this report and ensure we take further actions to progress towards the targets set."

POL00423567

Digital Identity – Change Assurance Review (Ref. 2018/19-25)

Needs Improvement

Sponsor:
Martin Edwards

Audit actions:

P1	0
P2	8
P3	1
Total	9

Digital Identity is a strategic programme set to deliver a core digital identity platform which will allow customers to set-up and maintain re-useable digital identities and to query the identity-related information via APIs. This would enable the increase of GOV.UK Verify market share, enable solutions for passport and employment vetting and prioritise further developments to expand the digital business beyond 2019/20, an area with estimated annual market size of around £1.5bn to £2bn.

This change assurance review, assessed the effectiveness of the programme's controls with particular focus on programme initiation, requirements assessment, planned delivery of the core platform, as well as being a pilot for Change Excellence OBW2.0 methodology.

We have highlighted many areas of good practice and observed improved change maturity as compared with previous Change initiatives. However, some improvements in the programme are required, with the result that this programme has been rated 'Needs Improvement':

- The programme is operating at risk – it has not executed agreements with its key delivery partner Digidentity (Digi), nor has it confirmed the costs of integration of two key application management services, the HR Vetting and Passport Renewals service offerings, with other third-party solution providers such as Atos, Accenture or Fujitsu. It also needs to engage further with the wider Post Office business and its vendors to ensure there is capacity to support the planned work.
- Although piloting OBW 2.0 and driving an Agile delivery method, its solution providers and the wider Post Office do not completely adhere to Agile, and require detailed level solution designs to mobilise, thus limiting its effectiveness of Agile delivery and adding additional challenges to the ambitious timescales that were set. Further the programme needs to plan to transfer the expertise of the contractors to the BAU team as it is currently relying heavily on contractors.
- Assumptions relating to the projected revenue streams need to be regularly reviewed, as do the key indicators outlined in the business case, so management has sufficient oversight during delivery to take early action and remediate if required.

Management Comment provided by Martin Edwards

"I welcome the conclusions of this Change Assurance Report, which as expected from an early stage review have highlighted both instances of good practice and some specific issues which need to be addressed. On the latter I can confirm that actions have either already been completed (such as signing the development contract with Digidentity) or are now underway (such as regularly reviewing resources, benefits projections and key indicators). The early stages of the programme were hampered by some specific resourcing challenges for key roles (both the programme manager and solution architect had to be replaced for differing reasons), but the core team is now in place enabling us to address the remaining issues highlighted by the report.

More generally, the report highlights the tensions of attempting to run an Agile product development process when some of our external suppliers and internal approaches are still more aligned to traditional Waterfall approaches. We will continue to work with SPO to ensure the broader learnings from this experience are captured."

POL00423567

Agent Remuneration (Ref. 2018/19-19)

Needs Improvement

Sponsor:
Debbie Smith

Audit actions:

P1	0
P2	4
P3	5
Total	9

The objective of this internal audit was to assess the design and operating effectiveness of controls in place over payments made to Post Office agents. Post Office has budgeted to spend £360m on agent remuneration in 2018/19.

Agent remuneration data was migrated from the SAP system to the Core Finance System (CFS) in February 2018 as part of the Back Office Transformation Programme. Agent details are maintained in and agent remuneration payments made through CFS. Agent remuneration is calculated monthly, based on rates stated in agent contracts.

Controls over the payment of agent remuneration were found to be well established and generally effective, although some control weaknesses were identified and areas for improvement have been highlighted. Specifically the audit identified that balance sheet reconciliations had not been completed consistently and requests to change agents' bank account details were not always independently validated.

The audit also highlighted that inputs to the agent remuneration process come from several teams in different locations and there are opportunities to improve the collaboration between them. Further, there is an opportunity to systemise the majority of the underlying agent records (joiners, movers and leavers documentation) as considerable reliance is currently placed upon paper based records to provide the audit trail of activities in the teams.

Management Comment provided by Tom Moran

"I am grateful to the IA team for conducting this audit and delighted to see such a positive assessment of Agent Remuneration, which is a direct reflection of the hard work of those responsible. I agree with and support the prompt implementation of the activities identified in the actions."

Internal Audit reviews planned for Q1 of 2019/20

10. The following reviews are being planned for Q1 (A full summary of the 2019/20 audit plan status is included in Appendix 2):

	Review	Status	Timing
1	Pensions Process (Follow-up)	Fieldwork	07/05 – 24/05
2	Procure to Pay	Planning	13/05 – 07/06
3	Telco Billing Process	Planning	10/06 - 28/06
4	Payment Technology Upgrade (PCI Compliance) (Change Assurance)	Planning	21/05 – 14/06
5	Digitising Mails (Change Assurance)	Planning	17/06 – 05/07
6	POI – Change Capacity	Planning	17/06 – 05/07
7	POI – AR Oversight (Phase 2, Operating Effectiveness)	Planning	17/06 – 05/07

POL00423567

Updates on Internal Audit Open and Overdue Actions

11. Audit actions are generally being completed on time. As at 30 April 2019 there were 21 open actions, none of which were overdue.

Audit Action Status:	BAU	Change	Total
Open (not yet due)	21	0	**21**
Overdue (<60 days)	0	0	**0**
Overdue (>60 days)	0	0	**0**
Total	21	0	**21**

END OF REPORT

POL00423567

Appendix 1

2018/19 Internal Audit Plan – Re-prioritised (ARC approved 30 Oct 2018) - Status as at 2 May 2019					
No.	**Title/Subject**	**Sponsor**	**Original / Addition**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	Product Risk Review (Postal Orders)	O. Woodley	Original	April	Needs Improvement
2	Employee Expenses	A. Cameron / M. Kang	Original	April	Unacceptable
3	Procurement Fraud Investigation	A. Cameron	Addition	May	Not Rated
4	Month-end Close Process	A. Cameron	Addition	Nov	Satisfactory
5	MoneyGram Compliance	O. Woodley	Addition	Sept	Satisfactory
6	Contract Management (IT)	R. Houghton	Original	Oct	Final Draft Report
7	Whistle-blower Process	J. MacLeod	Original	Oct	Satisfactory
8	Opening of Bank Accounts	A. Cameron	Addition	Nov	Satisfactory
9	FS Training & Competence	O. Woodley	Original	May	Fieldwork
10	Cyber Security	R. Houghton	Original	Jan	Not Rated
11	IT Control Framework	R. Houghton	Original	March	Draft Report
12	Financial Control Framework	A. Cameron	Original	Jan	Final Draft Report
13	Payroll	M. Kang	Original	Feb	Final Draft Report
14	Client Settlements Process	A. Cameron	Original	Jan	Satisfactory
15	Agents Remuneration	A. Cameron	Original	Jan	Needs Improvement
16	Network and SGEI Reporting	D. Smith	Addition	Feb	Needs Improvement
17	Procure to Pay	A. Cameron	Original	Q4 / Q1	Postpone[2]
18	Branch Cash Forecasting & Management	A. Cameron	Original	Q1 19/20	Postpone[1]
19	Supply Chain Management	A. Cameron	Original	Q1 19/20	Postpone[1]
20	Digital Strategy & Capability	O. Woodley	Original	2019/20	Postpone[2]
21	Online Sales	O. Woodley	Original	2019/20	Postpone[2]
22	Data Privacy (GDPR Follow-up)	J. MacLeod	Addition	Q1 19/20	Postpone[2]
Change Assurance[3]					
1	Change Excellence (Trafalgar)	R. Houghton	Governance	May	Advisory Report
2	DMB Strategy	D. Smith	Programme	July	Satisfactory
3	Branch Hub (Agents Portal)	D. Smith	Programme	October	Needs Improvement
4	Investment Funding Controls	R. Houghton	Governance	November	Needs Improvement
5	Payzone Integration (Panther)	D. Smith	Programme	Jan	Final Draft Report
6	Digital Identity Services	M. Edwards	Programme	Feb	Needs Improvement
7	Digitising Mails	D. Smith	Programme	TBC	Postponed to 19/20
8	Payment Technology Upgrade (PCI)	D. Smith	Programme	TBC	Postponed to 19/20
9	Change Excellence (Follow-up)	R. Houghton	Governance	March	Final Draft Report
10	P2C Belfast Exit	R. Houghton	Programme	March	Final Draft Report

[1] Delay until after BOT programme is complete and new controls embedded.

[2] Postpone due to process still bedding down and maturing (GDPR) / restructuring (Digital & Online) / remediation (P2P).

[3] The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2018/19 at the time. The list is being reviewed and updated on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum' projects.

POL00423567

Appendix 2

2019/20 Internal Audit Plan - Status as at 2 May 2019					
No.	**Title/Subject**	**Sponsor**	**Source**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	Procure to Pay	Interim CFO	Original	May	**Planning**
2	Branch Cash Forecasting	Rob Houghton	Original	Aug	Not started
3	Supply Chain (CViT)	Rob Houghton	Original	Aug	Not started
4	Accounts Receivable	Interim CFO	Original	Flex	Not started
5	Agent On-boarding	Debbie Smith & Rob Houghton	Original	Q4	Not started
6	Pensions Follow-up	Mo Kang	Original	May	**Planning**
7	Employee Expenses Follow-up	Mo Kang	Original	July	Not started
8	Branch Banking Framework	Debbie Smith	Original	Q3	Not started
9	Sales (Savings Accounts)	Owen Woodley	Original	Q3	Not started
10	Vetting / Fit & Proper	Ben Foat & Rob Houghton	Original	Flex	Not started
11	Effectiveness of Risk Management Framework	Interim CFO	Original	Flex	Not started
12	CFS Controls (Post BOT)	Interim CFO	Original	Q2	Not started
13	Effectiveness of Compliance Function	Ben Foat	Original	Flex	Not started
14	Telecoms Customer Billing	Owen Woodley	Original	June	**Planning**
15	Data Privacy (incl. follow-up of GDPR)	Ben Foat	Original	Q1	Not started
16	Cyber Security Follow-up	Rob Houghton	Original	Q2	Not started
17	Payzone Control Framework	Debbie Smith	Original	Q2	Not started
18	FS Branch Sales	Owen Woodley & Debbie Smith	Original	Flex	Not started
Change Assurance[1]					
1	Investment Funding Controls follow-up	Rob Houghton	Governance	Jul / Aug	Not started
2	Effectiveness of 2nd line Programme Assurance	Interim CFO	Governance	tbd	Not started
3	Benefits Realisation (Product Realisation)	Rob Houghton	Governance	tbd	Not started
4	Portfolio Level Operational effectiveness (excl. assurance, and gating process)	Rob Houghton	Governance	tbd	Not started
5	Effectiveness of the Gating Process	Rob Houghton	Governance	tbd	Not started
6	Belfast Exit (phase 2)	Rob Houghton	Programme	Sept	Not started
7	Data Governance Programme (Record management)	Rob Houghton	Programme	tbd	Not started
8	PTU (PCI Compliance)	Rob Houghton	Programme	May	**Planning**
9	Digitising Mails	Debbie Smith	Governance	June	**Planning**
10	Identity Services (Follow-up)	Owen Woodley	Programme	tbd	Not started

[1]The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2019/20 at the time. The list is being reviewed and updated on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum' projects.

POL00423567

RCC 9 May 2019

Addendum to Internal Audit report

Financial Controls Framework (Ref. 2018/19-21)

Needs Improvement

Sponsor:
Al Cameron

Audit actions:

P1	0
P2	6
P3	1
Total	7

This audit covered 12 of the 17 financial processes in the Financial Controls Framework., with the remaining 5 processes being covered through separate deep dive reviews. The audit also assessed the effectiveness of the control self-assessment process through the TrAction system.

We concluded that the controls within the framework continued to operate effectively for the most part. However, the large amount of controls work carried out in preparation for the Back Office Transformation (BOT) programme and the ongoing improvements have highlighted limitations with the TrAction system, which had impacted the effectiveness of some controls. TrAction is not readily configurable to provide all the required functionality and does not provide sufficient visibility over the 2nd line of defence activity (specifically the resolution process where control deficiencies have been identified). BOT also impacted resource availability, which in turn, temporarily reduced the effectiveness of the 2nd line oversight and resulted in a lower controls maturity compared to previous years (71.8% controls were effective, vs. 78.8% the previous year). As a result, we have rated this report '**needs improvement**'.

Management Comment provided by Micheal Passmore

"The report is fair and representative of the system limitation issues experienced, which was highlighted at the time the system was chosen. The system limitations have caused significant manual workarounds to ensure accurate monitoring and reporting, and we are now investigating alternative solutions. Until such time we will focus on the issues we can address, increase manual workarounds and continue the education process to the business."

POL00423567

Risk Report

Author: Jenny Ellwood Sponsor: Jane MacLeod Meeting date: 09 May 2019

Executive Summary

Context

This paper provides an update on the key and emerging risks the Post Office is managing.

5.1

Questions this paper addresses

- What are the key risks facing the business 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?
- What is the latest on risk exceptions and incidents?
- What is the latest position on AML/Financial Crime risks?
- What is the status of the Change Portfolio, its current top portfolio risks, delivery status and key delivery challenges?

Conclusion

- The paper provides an update on 4 of the 5 key risks reported in March as they remain relevant today: PCI, Information Security, Litigation and Change Workforce. The risk of a 'No Deal' Brexit has been deferred to 31 October and confidence has increased in terms of how we would manage a 'No Deal' scenario. That said the extension and the problems faced in agreeing a deal does increase the possibility of a general election. In light of this a review of the report to the Labour Party by the Communication Workers Union and Democracy Collaborative on 'A new public Banking Ecosystem' is being reviewed. An update is provided within the emerging risk section.
- One new exception has been approved since March RCC relating to the contract renewal of SuccessFactors. The number and type of significant incidents have followed a similar trend as previous months.
- In terms of emerging/future risks we are preparing the business for an effective immediate and short term response to the Horizon Trial phase of the GLO proceedings. We also note the challenge of people risks following recent and planned structural and organisational design changes. Additionally, we are maintaining a watching brief on the Loyalty Super Complaint and Treasury's consultation on the public sector redundancy cap.
- The risk profile for AML is currently amber and we have recommended that we do not separately categorise from Financial Crime. The results from a series of Financial Crime workshops will be reported in July.
- For Change Portfolio the number of programmes reporting a red status has slightly increased. The overall performance view remains amber.

Input Sought

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

POL00423567

The Report

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

1. There has been moderate change to the heatmap status confirmed in March (see Appendix 1). A principal risk on third parties is now incorporated and has been populated for each Business Area. As indicated by the heatmap Legal and Regulatory and Strategic are the principal risk categories which are reported red and where there is continued focus on actions.

2. The latest PCI Programme update forms part of this month's RCC. From a risk perspective, we report that 80% of the data discovery is complete (to be finalised by June). Positively, to date there have been minimal instances of card data being held across the network. The current position is that there are two linked areas for the ROC; payments and banking. Both require remediation to become PCI compliant. A plan to achieve both has been communicated by November 2020, but work continues to bring this forward.

3. Risks exist in the agreement with Global Pay but positively, our contract has been recently renewed for another 12 months. Communications between PO, Global Pay and our wider banking framework is key. It is also noted that the Programme have identified a potentially simpler and faster solution involving 'outsourcing' our payments methodology and are working with key partners to understand what may be possible. However, as at this point the Programme will not deliver the original plan or the potential new solution within the originally communicated timelines. As such, we do not believe that the risk position has changed yet, and it remains as 'High, 16'.

4. IT Security's 19/20 Security Improvement Plan is progressing. Engagement with a new third party (Recorded Futures) has introduced new threat monitoring/dark web scanning and a password complexity tool across POL estate, ensuring colleagues use stronger passwords.

5. Within the Strategic category Brexit risk remains but the impact of a 'No Deal' has been delayed to the end of October. Our confidence in managing any impacts in the event of 'No Deal' has increased as we were ready to deploy contingency plans at the end of March and then the middle of April.

6. Additionally, under Legal and Regulatory elements of the heatmap, the Banking Director has flagged that there has been heightened interest from the banks regarding card withdrawal card transactions. Point of sale card transactions carry a merchant charge whilst cash withdrawal card transactions does not and also creates an increase in remuneration for the Postmaster. Given this there is a risk that the transactions are not being processed correctly by the Postmaster.

POL00423567

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

7. In terms of Litigation risk, a range of activities are being mobilised as part of an Operations Transformation Programme. The programme is organised into 4 value streams which reflect the end to end lifecycle of an agent with a full business case expected to be ready by the end of June. In summary, however, and in addition to being more transparent in everything we do and sharing more information with Postmasters, the programme is also looking to better help people: open Post Offices, work in Post Offices; and manage Post Offices.

8. The second trial relates to Horizon and is pending direction from the Court of Appeal on the Post Office's application to recuse the managing judge. The trial is to resume on 4 June and conclude in the week commencing 1 July. We have asked Teneo Consulting, who has relevant experience in crisis preparedness and response work (e.g. working with RBS on the Global Restructuring Group losses issue; Oxfam on Haiti allegations of child abuse by aid workers), to assist us prepare for a potentially adverse judgment on Horizon issues.

9. Teneo will hold individual and group sessions to surface all relevant concerns, and help the teams to develop sensible mitigations both in the individual and aggregate. We anticipate this work will be complete by mid-June, leaving us some time to refine plans prior to the earliest possible date for judgment (which is likely to be before mid to late Summer 2019).

10. There have been significant people changes in critical roles and further organisational design changes are planned. A paper on succession planning is being presented to the Board in May to consider capacity required from GE-1 to step into such roles. We will further consider whether there are any wider risks from the changes, particularly from a governance perspective.

11. The Brexit delay does create more uncertainty and the possibility of a general election is still being discussed. With this in mind a review of the report to the Labour Party by the Communication Workers Union and Democracy Collaborative 'A new public Banking Ecosystem' is being considered. The document sets out recommendations relating to a new banking system. Those which would most significantly impact our strategy and operating model include:
    - creation of Post Bank to provide a full range of retail banking services through the Branch Network
    - Post Bank would be separate legal entity that will pay an annual access payment to Post Office for use of assets
    - Probable ending of our partnership with BOI
    - the range of financial products and services currently offered through Post Office Money to be transferred to Post Bank
    - Post Bank would seek to acquire the existing BOI UK portfolio

POL00423567

12. A watching brief remains with the Loyalty Penalty Super Complaint and the pricing and product proposition risks which this may create if the ruling is not in favour of Financial Services

13. In April, Treasury launched a consultation outlining how ministers will introduce a £95k redundancy cap on pay outs for public sector workers. We will look to consider the impacts of this with HR.

14. In March we advised work had commenced on how we can improve to identify and manage risks arising from change but manifesting themselves within the business. This is focused on clearly articulating the adverse impact that the change could introduce to the business through (but not exclusively) unforeseen operational change, delay, cost overrun and/or failure to realise the benefits of change. Work is still in its early stages but we are already ensuring, for example, analysis undertaken in our joint project-business workshops (e.g. PCI compliance, Digital Identity), health checks (e.g. Horizon Integration Hub) and post implementation reviews (e.g. Enhanced User Management) keep in mind such issues and, where appropriate, the associated outputs reflect the required action.

What is the latest on risk exceptions and incidents?

15. One exception has been approved since March RCC relating to the renewal of SuccessFactors outside of Public Procurement Regulations 2015. A Renewal Order Form was completed (as legally advised) to mitigate the risk of procurement challenge. The intention is to carry out an open procurement through G cloud in the next 9 months.

16. Significant incidents have continued in a similar trend in March, with Branch Network ATM gas attacks and data privacy breaches forming the majority of the reporting. Overall year to date volumes are consistent with 2018. Enhanced incident reporting is in future development and focused on the key themes and trends to support Committee action to formally pick up and fix, to highlight the gaps in business reporting and to reduce the recurrence of similar incidents where possible.

What is the latest position on Financial Crime?

17. In the January 2019 ARC, the Central Risk team was asked to consider the severity of AML and whether this would lend itself to be listed separately from Financial Crime as a principal risk on the risk heatmap.

18. There has been significant improvements to the control environment for AML which is now an amber status. These improvements include stronger mandatory compliance training and gaining access to all 'bureau de change' data for transaction monitoring and profiling, leading to a 4-fold rise in identification of issues since it was introduced end June 2018. We recommend not to separately categorise AML at this time.

19. We previously informed the Committee that we anticipated a commencement of a series of Financial Crime Workshops. We plan to carry out these out in

POL00423567

May as a joint activity with the Financial Crime team, identifying any gaps in risks profile with the focus of embedding accountability and responsibility as well as getting a better understanding the significance of AML to Post Office within the holistic Financial Crime category principal risk. These results will be brought back to Committee in July.

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

20. The overall status of the portfolio is unchanged at 'amber'. By P12, actual realised benefits for 2018/19 were £37.5m (6.7% below baselined plan). The overall portfolio continues to be prioritised to ensure benefits over the next 3 years are secured. By P12 actual 2018/19 investment was 'amber'. Although the end year position was in line with the revised 9+3 forecast it actually exceeded the original 2018/19 budget. Portfolio prioritisation for 2019/20 has been revisited to ensure there is appropriate focus on GLO outcomes along with recommendations from the McKinsey work on a new target operating model.

21. In 2/2019 we launched enhanced assurance activity including improved the piloting of formal health checks on specific 'Gold' and 'Platinum' programme/projects. The latter was piloted on Data Analytics and GDPR. A further health check is being completed on Horizon Integration Hub and a further 3-4 have been identified between 5-6/2019.

22. A summary of the current key 'Platinum and Gold' change programmes and their current reporting status is provided at Appendix 2. 7 projects are reporting Red RAG status. Key ones are:
    - Back Office Transformation (All RAG statuses Red): Multiple red statuses reflects the uncertainty in Cash Reconciliation. Back Office Transformation went live at the end of 2/2019 and POLSAP is now only an archive. Positively the financial team have closed P11 and are close to closing the P12 with little issue. Early life support will end in 5/2019 with this project element then closing. However our Supply Chain team still face operational challenges. The key issue remains Cash Reconciliation although this is improving. At this point it is uncertain when this project element will close. The programme intend to provide a Board update in 5/2019 with an estimate to complete.
    - Data Analytics (Benefits and Risk Red RAG): Programme funding significantly reduced in prioritisation. Programme is now being changed with data governance and MI moving into BAU. Programme now working with POI to deliver a POL-wide 'Data Lake' architecture. This is to be scoped within 6/2019 which will improve the RAG rating.
    - PCI Compliance (Benefits, Delivery, and Risk Red RAG): The reason for the status of this programme is covered in paragraphs 2 & 3. We expect the solution to be agreed by the end 4/2019, with costs and timetable confirmed early 5/2019. Point to Point Encryption (P2PE) remains a key PCI deliverable with deployment across the pin-pad estate.
    - Legal Entity Optimisation (Cost, Delivery & Risk Red RAG): 12 week KPMG assurance work began in early 4/2019, following which scope for LEO can be re-baselined with UKGI. Target mid-7/2019 to agree scope.

POL00423567

Change Workforce

23. At its meeting in 4/2019, CRMG continued to consider there was 1 change related portfolio risk for the RCC/ARC to note (Change Workforce). Although initially referred in 1/2019 the mitigations have been more developed. The Strategic Portfolio Office (SPO) are starting to collect resource profiles to build a view of experience and skills. These will eventually be uploaded into Service Now (the portfolio enterprise management tool). The Competency framework is ready to be deployed at an appropriate point. Communities of Practices continue to provide further professional support. Whilst we consider, for this reporting period, the current RAG rating remains unchanged, there is a decreasing trend in risk severity and likelihood which should manifest itself in the next update, see Appendix 3.

POL00423567

Appendix 1. Heatmap

Principal Risks	Trend / Risk Green Status Expected Date	Retail	FS&T, Identity and POI	Finance (CFO)	Operations (COO)	Legal, Risk and Governance	IT	HR (incl. H&S)	COMM	ALL	May-'19 Comments
Operational	Mar-'19						↑			n/a	**Red** – No high concerns reported in this area. There is one new key risk for Banking Services related to LINK Disaggregation, where LINK will stop supporting settlement by 1st July 2019. Options are currently being discussed to mitigate this risk. **Key Amber points** – The Safety Compliance Top Risk remains 'Amber' as improvements to H&S training and compliance are ongoing. . For Network Operations, work continues on creating a Branch Support Centre in Chesterfield to replace the current NBSC helpdesk model.
	May-'19	↑				↓	↔			n/a	
Information Security	Mar-'19									n/a	**Red** – Whilst Info Security is not called out red, Cyber Threat will remain a focus area and forms part of our top-risk profile. **Key Amber points** -The Deloitte Cyber Report has now been published and remediation activities will continue throughout the year. The risk profile will remain 'Amber' until material changes in the remediation programme have been approved by Audit.
	May-'19									n/a	
Technology	Mar-'19									n/a	**Red** – No business area is currently reporting high concerns in this area. Retail continues to hold a key risk around the failure of IT infrastructure in branch, reflecting the importance to ensuring branches can continue to trade. **Key Amber points** – For FS&T, Identity and POI, the overall risk status has moved to 'Amber'. This is predominately to do with our legacy IT systems e.g. Horizon. Alongside this, the development of the Digital & Identity strategic plans are currently underway. For IT, CC have advised that the current version of software which connects service for branch and admin users is currently out of date. Priority to upgrade the critical services will be discussed at the architect review which is scheduled to take place this week. The Fujitsu campus failover is scheduled to take place at the end of May which will reduce the overall risk in the IT DR landscape.
	May-'19		↑				↑			n/a	
Third Party	Mar-'19	New risk subcategory to be assessed for RCC in May 2019.									**Key Amber points** - For FS&T there is one key risk over Telco Third party exposure. We are reliant on Fujitsu's guarantee that they are compliant with Regulations and Law. We are now in contractual negotiations and plan to start a tendering process. In IT, currently 3 contracts are out of support that could potentially impact the speed of resolution for incidents impacting Finance Operations (Credence/MDM application IBM support, Credence/MDM application Oracle support and SAP Business Objects). Remediation plans are under review.
	May-'19						↑			n/a	
Legal & Regulatory	Mar-'19	Re. PCI ↑	↑			Re. PCI ↑	Re. PCI ↑			n/a	**Red**- The risk score for PCI has remained the same. 80% of the data discovery is complete and is due to end by June 19. POL's current position is that there are two linked areas for the ROC; payments and banking. A plan to achieve both PCI Compliance has been communicated as November 2020, but work is underway to identify a more aggressive timeline. For Banking Services, there is one new key risk related to a non-conformance in cash withdrawal card transactions without advising or requesting the customer for approval. It helps the PM avoid a POS Merchant charge and instead creates a remuneration increase. A technical solution has been requested to Fujitsu/ATOS to eliminate the issue. FS&T Regulation remains a concern for Telco and this has moved the risk profile from Amber to Red, due to a key person dependency. **Key Amber points** – For HR, 'Employment Practices' remains 'Amber', ER training will be piloted at the end of May and will roll out in June which should mitigate this risk. Will be unlikely to see actual risk benefits in the immediate term.
	May-'19	Re. PCI ↑	↑			Re. PCI ↑	Re. PCI ↑			n/a	
	Risk Green Status Expected Date	Nov-20				Nov-20	Nov-20				
Financial	Mar-'19		↑							n/a	**Key Amber points** – In FS&T there is a key risk over Ofcom pricing differential review that remains a concern for Telco. Telco compliance manager met with Ofcom in March to lobby from Post Office point of view. Now awaiting consultation before commencing further lobbying. One key risk has been closed in respect of inadequate financial controls for FS&T. For IT, FY18/19 results closed at £91.8m, (£2.4m off budget). The cost challenges were due to delays in Project Everest Belfast Exit, savings expected through contract negotiations fell short of target and savings from networks migration lower than anticipate.
	May-'19		↔							n/a	
Strategic	Mar-'19									Brexit	**Red** - 3 POL Top Risks (Retail) Proposition, (FS&T) Market Developments and Brexit Implications. Work continues on developing the Retail Proposition to provide greater access to Post Office products and services. The Corporate & Market Developments risk remains Red. Projects and negotiations underway with BOI, RMG and development continues with digitisation for PO. Brexit - Confidence increasing into how we would manage contingency in the event of a 'No Deal', but political uncertainty remains.
	May-'19									Brexit	
	Risk Green Status Expected Date	31-Oct-19	31-Oct-19							31-Oct-19	
People	Mar-'19		↔							n/a	**Key Amber points** - For the Digital Competency Risk, work is underway to support the Digital Workplace Programme (delivered by IT), whereby HR focus on development of Talent Acquisition and Development Programmes. Further review is required on the scope of this activity and feedback from a recent review by McKinsey being considered. In FS&T and Identity the impact classification has moved to 'worsening', due to the recent loss of colleagues across various businesses:
	May-'19		↑	↓						n/a	
Change	Mar-'19								n/a		**Key Amber points** - In IT change portfolio prioritisation and execution continue the process of assessing the change agenda and determine IT priorities. Change portfolio tracking remains 'Amber' primarily because 18/19 secured benefits were 6.7% below plan and 18/19 investment was above original budget. 7 out of 37 'Platinum' and 'Gold' programme/projects reporting Red RAGs. These are Fit & Proper, Back Office Transformation, Data Analytics, Future of POCa, Digital Identity, Legal Entity Optimisation and PCI Compliance. Top 3 remain Portfolio performance, change workforce and business ownership. Significant independent ongoing review of programme risks logs – demonstrates broad compliance with standards but improvement required in specific areas.
	May-'19								n/a		

↓ Improving ↑ Worsening ↔ Stable

POL00423567

Appendix 2. Change Portfolio: Gold & Platinum programme/projects dashboard[1]

			RAG status				
Business Unit	Project Name	Investment Type	Cost	Benefits	Delivery	Risk	Overall
F&O	Process & Contact Centre	Cost Reduction	Amber	Green	Green	Amber	Green
F&O	Project Arrow -Data & Analytics	Strategic Enabler	Amber	Red	Amber	Red	Amber
F&O	Source to Settle	Cost Reduction	Green	Green	Green	Green	Green
F&O	Safe Haven Exit	Cost Reduction	Green	Green	Amber	Green	Amber
F&O	Future of Stock	Cost Reduction	Green	Green	Green	Amber	Green
F&O	Back Office Transformation	Cost Reduction	Red	Red	Red	Red	Red
F&O	Branch Hub	Cost Reduction	Green	Amber	Amber	Amber	Amber
F&O	Agent On boarding	End-User experience	Green	Green	Green	Amber	Amber
F&O	Common Services	Strategic Enabler	Amber	Green	Amber	Amber	Amber
FS&T	Home Phone & Nuance	Cost Avoidance	Green	Green	Amber	Green	Amber
HR	Success Factors – Phase 2	Strategic Enabler	Green	Green	Amber	Amber	Green
HR	Blueprint	Cost Reduction	Green	Green	Green	Green	Green
Identity	Digital Identity	Strategic Enabler	Green	Green	Red	Amber	Amber
IT	PCI Compliance	Cost Avoidance	Amber	Red	Red	Red	Red
IT	Project Everest	Legal & Regulatory	Green	Green	Green	Green	Green
IT	Belfast Exit	Cost Reduction	Green	Green	Amber	Green	Amber
IT	Security Operations Centre	Strategic Enabler	Green	Green	Green	Green	Green
LRG	Legal Entity Optimisation	Strategic Enabler	Red	Amber	Red	Red	Red
LRG	Fit & Proper	Legal & Regulatory	Green	Amber	Amber	Red	Amber
LRG	General Data Protection Regulation	Legal & Regulatory	Amber	Green	Amber	Green	Amber
Insurance	Nemesis (Home)	Strategic Enabler	Green	Green	Amber	Amber	Amber
Insurance	Morpheus (Pricing / CVM)	Strategic Enabler	Green	Green	Green	Amber	Amber
Retail	POCA Implementation	Service Sustaining	Green	Green	Amber	Green	Amber
Retail	Horizon Integration Hub	Strategic Enabler	Green	Green	Green	Amber	Amber
Retail	Enhanced User Management	Legal & Regulatory	Green	Green	Green	Green	Green
Retail	SSK Trial	Strategic Enabler	Green	Green	Green	Green	Green
Retail	Network Development	Service Sustaining	Green	Green	Green	Amber	Green
Retail	Network Transformation	Service Sustaining	Green	Green	Green	Green	Green
Retail	Future of POCa	Revenue Generating	Green	Green	Red	Green	Red
Retail	Cheque Imaging	Legal & Regulatory	Green	Green	Amber	Amber	Amber
Retail	Crown Network Shape	Cost Reduction	Green	Green	Green	Green	Green
Retail	DMB Strategy	Cost Reduction	Green	Green	Green	Green	Green
Retail	Mails Multi-Channel	Revenue Protection	Amber	Amber	Amber	Amber	Amber
Retail	SSK Simplification	End-User Experience	Green	Green	Amber	Amber	Amber
Retail	Parcel Shop	Revenue-Generating	Green	Green	Amber	Green	Amber
Retail	Automated Locals	Revenue-Generating	Green	Green	Green	Green	Green
Retail	SSK Procurement	Cost Avoidance	Green	Green	Green	Amber	Green

[1] Data taken from Strategic Portfolio Office Change Monthly Executive Summary (P12) – April 2019

POL00423567

Appendix 3. Change Workforce risk

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
Change Workforce risk	The risk that incorrect resources (lacking the skills and capabilities) are assigned to change programmes. This would impact value and effective delivery. Workforce needs to be upskilled to obtain necessary skills and capabilities and costly recruitment will resolve short term gaps	**12** **I/L: 4:3**	Upskilling existing workforce: • Complete gap analysis and identity training development needs • Maintain Communities of Practice – to enable capability improvement • Stronger focus on raising performance bar –focus on SMART objectives + performance mgmt. Assigning right resources to projects: • Increased SPO challenge to project structure and role requests. Role reshaping where needed + removing project blockers to performance. • Staff biographies continue to be collected to build portfolio skills and experience picture • SPO Resourcing formalising 30, 60, 90 working day check-ins with hiring managers for feedback on individual contractor performance • Challenging contractor renewal against performance and competencies, converting high risk roles to FTC where possible • Reviewing and improving existing resource practice. • Deployment of Service Now-resource management tooling is being built. Deployment in will be against other priorities. Evolving roles/capabilities for agile/digital • Defining new roles and competencies + standard agile JDs. • Agile Centre of Excellence – project set up, training/coaching - Intranet page with guidance	5-6/2019 Ongoing 6/2019 By 5/2019 tbc Complete Complete In progress 6/2019 (tbc) In progress In progress	**3** **I/L: 3:1**

POL00423567

Appendix 1

POST OFFICE

GROUP RISK PROFILE - May 2019

Post Office Top Risks

Business Area	Principal Risk	GE Risk Owner	#	Risk Description	Inherent Risk Score (I/L)	Key Controls in place	Controls Effectiveness Score	Residual Risk Score (I/L) Mar-19	Residual Risk Score (I/L) May-19	Movement	Rationale for Movement / Mitigation Plan
LRG / IT	Information Protection & Regulatory Compliance	RH/IMaC	1	**PCIDSS** The 2017 PCI Audit identified a number of Audit Actions across 3rd party IT suppliers which are "not yet compliant". Failure by Post Office to address these findings and provide a robust plan to resolve the actions (within an estimated timescale of 12 – 24 months) may result in challenges during external audits, operating restrictions or financial penalties from partners, require remediation activities and attract unbudgeted remediation costs.	5 - 3	IT Project in place to address the requirements for certification. Formation of PCI Steerco Stop, Start, Continue assessment has been completed to identify forward plan Potential plans to certification have been reviewed. Gap Analysis has been completed to identify a potential reduction in scope and deliver a Mediated RoC	2	4 - 4	4 - 4	⇨	**Rationale for Movement** The risk position has not changed since our last report, and it remains as 'High, 16'. From a risk perspective, we can report that 80% of the data discovery is complete and is due to complete by June 19. Positively, there have been minimal instances of card data held across the network. The conclusion of the discovery will define PO's PCI scope. The current position is that there are two linked areas for the ROC; payments and banking. Both require remediation to become PCI Compliant. A plan to achieve both has been communicated as November 2020, but work is underway to identify a more aggressive timeline. **Mitigation Plan** 1) Principle design 2) Customer transactions being remediated - Retail transactions – for payment transactions via credit card 3) Customer transactions being remediated - Banking transactions – for cash withdrawals, balance enquiries, pin changes and deposits 4) Customer transactions being remediated - Bill payments and non-chip and pin transactions – for transactions where a customer wishes to pay a utility bill for example, the barcode on the bill is scanned and this often includes the PAN number for use in transaction execution 5) Deployment has commenced and pin-pads will be shipped back to the supplier, Ingenico. The PCI compliant software will be installed and the devices redeployed back to all our branches over a period of 7 months. 6) Eliminate PAN data from Post Office back end systems 7) PCI Card Data Scan 8) Pre-Pay and Post Office Branded Cards 9) External Client and Branch Communications
Retail	Competitiveness, Market and Customer Relevance	DS	2	**Retail Proposition** Post Office's retail value proposition becomes insufficiently attractive to retailers which results in shrinkage to our branch network and breach government commitments. This is potentially compounded by increased costs associated with Brexit.	5 - 4	The Retail Strategy presented to the Board in June contains three pillars of activity, particularly better franchise relationships, which will address this point. Also close account management of government relationship through regular updates on network numbers and trends.	2	5 - 3	5 - 3	⇨	**Rationale for Movement** No change in the risk score this quarter. **Mitigation Plan** Work continues on developing a new segmented proposition tailored to Agents and provide greater access to Post Office products and services through a range of devices owned and operated by retailers, customers and the Post Office. A technical proposition tailored to our multiple partners is due to be rolled out this quarter to enable Lottery sales on retailers' tills. Other developments in this quarter include 15 pilot locations for Post Office Parcel Shop due to go live in June 2019. Work also continues on automated locals, with the first proof of concept branch expected to go live in June 2019.
LRG	Litigation	JMaC	3	**P.O Group Litigation** Adverse outcome from current Group litigation.	5 - 3	- PO has in place a Steering Group with attendees from across the business with appropriate level of seniority to ensure that the resource, decisions, materials and documentation necessary for PO to be able to robustly defend its position are available to it; - External Legal Team (including Senior Counsel) keeps PO's position in the litigation under constant review; - A Board Sub Committee has also been established to oversee the litigation and respond to its risks; - Contingency Planning work is also undertaken to respond to the litigation risks.	3	5 - 2	5 - 3	⇧	**Rationale for Movement / Mitigation Plan** Judgment on the first 'common issues' trial was given on 15 March 2019, and made findings adverse to Post Office's interests and business as usual operations. Therefore the risk score has moved to 5x3 this refresh. **Mitigation Plan** 1) A range of activities are being mobilised as part of an Operations Transformation Programme. The programme organised into 4 value streams which reflect the end to end lifecycle of an agent with a full business case expected to be ready by the end of June. 2)We have asked Teneo Consulting, who has relevant experience in crisis preparedness and response work (e.g. working with RBS on the Global Restructuring Group losses issue; Oxfam on Haiti allegations of child abuse by aid workers), to assist us prepare for a potentially adverse judgment on Horizon issues 3) Teneo to hold individual and group sessions to surface all relevant concerns, and help the teams to develop sensible mitigations both in the individual and aggregate. We anticipate this work will be complete by mid-June, leaving us some time to refine plans prior to the earliest possible date for judgment (which is likely to be before mid to late Summer 2019).
IT/LRG	IT Security / Information Protection & Regulatory Compliance	RH/IMaC	4	**Cyber Threat** We have critical IT Security exposures highlighted by a third party (Deloitte) review across our security infrastructure. These relate to firewalls, pen testing and out of date infrastructure. We have mobilised a Security Transformation programme to mitigate this risk. Failure to adequately deploy and effectively manage data protection policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer).	5 - 5	**Internal** '- eLearning Module. - Information Security Governance. - 2018 Information Security Culture Campaign. - Engagement initiatives and targeted learning sessions in design and communications planned. **External** - IT Security polices have been refreshed and communicated - SOC Programme underway - Supplier Security meetings - Digital Shadows deployment providing cyber intelligence	3	4 - 3	4 - 3	⇨	**Rationale for Movement** No change in the risk score this quarter. In December 2018, Deloitte began the Cyber Maturity Audit. This has delivered a maturity report and recommendations for improvement over 34 domains. It is important to note that approximately 76% of the recommendations were already in the IT Security Improvement Plan for 19/20. Activities to resolve the recommendations have already commenced and are being tracked by Risk and Audit. IT have confirmed that the new CISO will start in May. **Mitigation Plan** 1) Increase the capability and cultural awareness around data protection 2) Improve the management and assurance of our third party suppliers 3) Extend the coverage and capability within our security operations. 4) Continue to extend Cyber security operations to ensure we have the necessary defence mechanisms in place to protect and react to any Cyber security exposures 5) Password strength tool implemented 6) Address and remediate all Deloitte security findings
Operation (COO)	BCP (excl ITDR)	RH	5	**DR / BCP plans** Limited DR/BCP plans, largely untested increase the impact of systems and site loss.	4 - 4	High level plans in place for Chesterfield and Bolton. Work area recovery tests for both Chesterfield and Bolton in April 2018 partially successful. Chesterfield test is planned 12th March 2019.	2	4 - 3	4 - 3	⇨	**Rationale for Movement** No changes to the risk rating, work remains ongoing, awaiting confirmation of contingency plans. **Mitigation Plan** The risk of business interruption due to inadequate BCP arrangements is unchanged from Q4 (4x3) reflecting incomplete DR testing at Chesterfield and Bolton and the need to install IT infrastructure in Swansea before Swindon can be tested.
HR	Develop, Inspire and Grow	MK	6	**Digital Competency** Failure to attract, retain and build the appropriate competence to address challenges posed by digital disruption shall lead to loss of customer base, fundamental disruption to the business model and eventual rapid decline of the business.	4 - 4	Providing digital tools in the workplace (Ben Cooke): Digital Workplace Programme Building capability and competency to use digital tools: a) Digital learning strategy in place; b) Providing skills through blended e-learning and F2F sessions across the business; c) SuccessFactors e-learning in place; d) Digital Stars network provides peer support (Yammer/Teams/training sessions). Attracting appropriately skilled talent (Sean): a) Working with CIO to identify additional channels to attract talent; b) Technology Graduate Programme launched.	2	3 - 4	3 - 4	⇨	**Rationale for Movement** No change in the risk score this quarter. **Mitigation Plan** 1) A review has been undertaken by Mckinsey who evaluate the current programme of work and inhouse capability to deliver the digital competency and the output of the review is being discussed. 2) Recruitment is underway for the new Digital and Innovation board (c15 new roles).

5.1

POL00423567

Tab 5.1.1 Appendix 1

Post Office Top Risks

Business Area	Principal Risk	GE Risk Owner	#	Risk Description	Inherent Risk Score (I/L)	Key Controls in place	Controls Effectiveness Score	Residual Risk Score (I/L) Mar-19	Residual Risk Score (I/L) May-19	Movement	Rationale for Movement / Mitigation Plan
FS&T	Competitiveness, Market and Customer Relevance	OW	7	**FS&T Market Developments/ Competition** Post Office faces both threats and opportunities to income from our competitive market place. Post Office operates under and extensive regulatory environment, covering areas such as financial and post services, telecoms, procurement and competition law and data security. This environment continues to evolve, we need to ensure that changing requirements continue to be identified and met. Failure to implement an effective strategy in response to these emerging markets, new entrants, market agility, business model changes, could result in our customer experience, propositions and channel strategy failing to deliver what customers want. We have difficult and uncertain negotiations with BOI, RM and Fujitsu within the 2018/19. Negotiations with key partners has the potential for increased costs on service and support. Substantial value share in BOI's favour, particularly FRES may weaken our profitability over time. This is likely to be the case if we remain constrained under the current relationship terms. Brexit has made the economic outlook even more uncertain. Low growth and confidence over spending will have negative impacts on our product areas in mortgages, insurance travel, savings and international parcels.	5 - 3	FS & T - Board and GE sign off on strategy agreed and being implemented. PO Money - Negotiations with BOI are ongoing - Head of terms agreed and working on contractual amendments. Digitisation -offer digital services including POGO & Digital Remittances. Telecoms - Agency initiatives to improve remuneration and incentivising them to sell product. Brand and market awareness. POI - Project NIKE currently underway. Strategic relationships and project delivery are key to product offering and growth for instance, Royal Mail Group and Bank of Ireland (UK) plc. Misalignment of strategic direction and focus with a partner could result in products that do not support our growth strategy or meet our customer or market requirements. Innovation - Digitation is changing the way consumers manage their finances and purchases. CHUB now moved into BAU and further development may be considered 2018/19(Mails on hold at present). New Post Office essentials app went l've in April 2019.	2	4 - 3	4 - 3		**Rationale for Movement** No change in the risk score since last review. **Mitigation Plan** Actions being taken are as follows: 1) PO Money - Negotiations with BOI are ongoing. Head of terms agreed and working on contractual amendments. Digitisation -offer digital services including POGO & Digital Remittances. Diversity of PO Money products through different product providers. 2) Telecoms - Agency initiatives to improve remuneration and incentivising them to sell product. Brand and market awareness. 3) POI - Project NIKE currently underway. 4) Strategic relationships and project delivery are key to product offering and growth for instance, Royal Mail Group and Bank of Ireland (UK) plc. Misalignment of strategic direction and focus with a partner could result in products that do not support our growth strategy or meet our customer or market requirements. 5) Innovation - Digitation is changing the way consumers manage their finances and purchases. CHUB now moved into BAU and further development may be considered 2018/19 (Malls on hold at present). New Post Office essentials app went live in April 2019.
ALL	Strategic	GE	8	**Appropriate actions for Brexit risks have not been considered** Brexit impacts and opportunities has been considered across PO, and appropriate actions and remediation activities are in development. A risk remains that Brexit could have a detrimental impact to PO's strategy, operations and infrastructure which are more prevalent in a 'no deal' decision.	4 - 4	Senior Management liaise with Government representatives on a periodic basis to ensure they are aware of the latest developments. POMS staff will liaise with PO staff to ensure that Brexit impacts and opportunities are considered. PO senior stakeholders working group has commenced in Sept 18 to establish the risks & opportunities post March 2019. Since the last review risk assessments have been completed across PO, providing a consolidated risk report of a 'no deal 'outcome. Legal have provided a BREXIT questionnaire which has been issued to our key suppliers.	2	4 - 3	4 - 3		**Rationale for Movement** No change in the risk score this quarter. The risk of a 'No Deal' has been pushed back to 31 October 2019. We are confident in how we would manage a 'No Deal' scenario. That said the extension and the problems faced in agreeing a deal does increase the possibility of a general election or another public vote. **Mitigation Plan** 1) Work with trade parties, the FCA and our key partners to understand the key risks of Brexit to our business. This work is ongoing. 2) Understand specifically how products will perform under Brexit scenarios e.g. long delays at ports or airports. 3) Understand any capacity issues or ongoing pass porting issues within our Insurance providers. 4) Look for opportunities as well as threats provided by Brexit. 5) Consider the implications for staff. 6) Consider how POMS will respond under stress scenarios if Brexit leads to a recession via falling pound, increased costs via tariffs or higher frictional costs. 7) Review Bank of Ireland no-deals plan, including availability of contact centres. 8) Review security procedures. 9) Confirm with insurers how they expect travel insurance to operate under No deal scenarios.
LRG / Retail	Litigation	JMaC / DS	9	**Sustainability of business model** The undermining of Agency status, as a result of either: CWU legal claims, Taylor review or from regulatory interventions is a new risk to watch given the fundamental impact to the sustainability of our business model.	5 - 3	Steering Group in place with attendees from across the business with appropriate level of seniority to ensure that the resource, decisions, materials and documentation necessary for PO to be able to robustly defend its position are available to it.	2	5 - 2	5 - 2		**Rationale for Movement** No change in the risk score this quarter. The business is monitoring the developments closely. The 3rd trial is underway, so no changes are expected until Oct/Nov 2019. **Mitigation Plan** A successful challenge is made with regard to the employment status of postmasters such that they are categorised as employees or workers and Post Office becomes liable for additional cost. This is being managed by HR with close involvement of our agents' Pay team (Nick Beal). It is also co-ordinated with our Horizon work (Same Leads).
IT	Technology Ops	BH	10	**Technology and Business Interruption** Post Office's network, and the products and services provided through that, are supported by and reliant upon complex technical architecture. There is a risk of failure of key systems or IT infrastructure reduces the effectiveness, availability, integrity or security of our Network. Direct impact on our network availability and reliability resulting in adverse customer service and financial performance and/or reputation.	5 - 4	1. Post Office has a Change Management policy that clearly defines what constitutes a change, how changes are raised, classified, prioritised, and how these changes should be processed by suppliers. 2. IT have a documented IT Service Continuity policy in place which caters for internal and outsourced business processes and service activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	2	3 - 3	5 - 2		**Rationale for Movement** The risk has been increased to 5x2. Impact has increased slightly as a result of the inability to failover automatically to the CC secondary datacentre. CC have confirmed that there are processes and procedures in place to perform a manual fallback in the unlikely event of a major disaster. **Mitigation Plan** 1) Upgrade to new Vsphere software. 2) Manual processes/procedures in place to perform manual fallback. 24 hours to implement. 3) DR fallover test to be rescheduled to October 2019.
FS&T	Compliance with laws and regulations	OW	11	**FS&T Regulation** There is a risk that the on-going increase in regulation in FS (and Telecoms businesses) increases the risk of non-compliance and/or making various business activities unprofitable (e.g., Insurance Distribution Directive and AML requirements). Regulatory risk from Ofcom activity e.g. review of general conditions, complaints, automatic compensation could lead to a drain on resources, increased costs to the business and impact on the change schedule.	3 - 5	Regulatory Horizon Scanning, compliance team resource to interpret and drive compliant solutions with different parties e.g., product teams, network, HR, training teams and Principals. Participation in Investment Committee Risk assessment of new initiatives, including completion of Customer Detriment Risk Assessments. Full review of the General Condition was completed for October 2018 to ensure that the changes made to the GCs were implemented. A check was done on existing GCs however there is reliance on Fujitsu. Further work is needed to get Fujitsu to provide evidence of their compliance.	2	4 - 2	4 - 2		**Rationale for Movement** No change in the risk score since last review. **Mitigation Plan** 1) We are working with our partners/suppliers and regulatory principals to ensure we have identified new/changes to regulations and have developed effective and affordable solutions on a risk-based approach 2) Part of the Law & Trends forum 3) Joined the CUI working group on regulation. 4) Weekly GC review meeting to discuss progress, expectation of this risk to materialise on the 7th of March 5) Change request is being raised to implement GC changes.
HR (incl. H&S)	Keep our people, customers and third parties safe	MK	12	**Safety Compliance** Safety outcomes are not world class and where they are not in line with required legal and regulatory standards, may lead to serious injury.	5 - 4	**Training** - H&S BPs continue to provide training to DMB, Supply Chain Managers and ANCMs and Training and Audit Managers and workshops for Safety Champions. H&S training has been converted to e-learning with support from the Learning Academy and issued in line with calendars. Additional training to be provided to CWU Reps, **H&S Audit** - HSL/ HSE have assessed the Safety Management System and reported that the PO SMS is level 4 (very good). A Safety plan identified 30 actions and safety Board monitoring to conclusion by year end. This includes enhanced training, more ownership and monitoring by middle managers and a review of risk assessments across business and evidence of compliance collated centrally. **H&S Activity Calendar** - H&S team are attending lead team meetings, DMB BDM meetings and wider Network Ops team meetings (ANCMs) to upskill managers in respect of their H&S responsibilities. **Property** - An independent assessment of high risk building fabric (including signage) is complete, with high and medium remedial works completed. **Road Risk** - An overarching Road Risk Policy has been developed and a final draft shared with stakeholders. An action plan has been agreed and a number of initiatives are being piloted for our driving communities.	3	4 - 2	4 - 2		**Rational for Movement** No change in the risk score since last review. **Mitigation Plan** **Training**: General H&S module content has been developed for issue in Q4/Q1 to all business except DMB and Supply Chain via Success Factors. Fire Awareness training was issued in November and driver training issued in Q4. There has been a much better uptake of this online training in 2018/19 and gaps are being closed. H&S BPs are attending lead team meetings to raise awareness across Network Ops and Support Teams. External IOSH Managing Safely training has been provided to 21 Safety Champions, H&S Lead for SC is booked on NEBOSH Certificate in March. CWU reps are attending H&S course and workshops to raise competence to ensure quality and consistent inspections. All CWU, Unite and H&S BPs attended joint workshop in February. Review of Supply Chain training will include a plan to deliver more face to face training in Q1 (19/20). **Higher risk activities** are being reviewed i.e. local Risk Assessments and safe systems of work e.g. use of tail lifts, use of machinery, stackers, loading and unloading. The H&S BPs are auditing and observing to assess risk and are also providing face to face training and coaching to line managers on site in Supply Chain and at high risk DMBs. **Compliance**: A H&S risk dashboard has been developed to include compliance and performance i.e. fire, training, risk assessments, accidents, across all business areas and shared at Safety Board and Ops Board. Certificates of Compliance are being completed and returned and activities monitored by H&S Team. Gaps are being shared with each 'H&S lead' responsible for compliance in that business area. **Road Risk**: E-learning training re-issued in Q4, reinforcing mobile phone whilst driving policy and over 500 drivers undertaken by February. We are consulting on the Alcolock COP for Commercial drivers. Working with BRAKE, RMG and possibly 3rd Pillar of Health to assess driving fatigue and distraction and provide advice and guidance to drivers and their line managers. **Property**: Low risk building fabric actions have been completed. Lozenges are being checked across c3800 local branches. Additional training, recognition, a review of procurement, contractor safety and risk assessment will be undertaken. An independent audit is being procured in Q1 19/20. Fire Risk Assessment remedial actions are 66% lower than previous year and are being closed with help from the H&S team and CBRE. **Security**: Investment Committee approved additional funding for a range of initiatives to reduce risk of robbery, including fogging at high risk branch counters, IP cameras as well as body cameras, security escorts and alarm upgrades.

5.1

2 of 2

POL00423567

Appendix 2

EXECUTIVE DECLARATION as at May 19

Principal Risk		Statement	Item No	Item	Identified by GE Member	ARA Action
TECH	Business Interruption (ITDR)	Material risks to Post Office that are not captured in the Group Risk Profile	1	**Transtrack - Application Architecture, Data Integrity and coding practice.** There is a current issue with Transtrack CWC, our cash inventory system. Cash movement transactions are recorded correctly in depots leading to a correct depot cash balance (confirmed through physical counts). However due to technical issues these do not all flow through to CFS our financial system. This has led to CFS being significantly understated. The Back Office Transformation project team have worked with finance (and our auditors) to maintain a log of all transactions missing from CFS and are able to evidence an accurate picture. This issue has exposed a risk that the Transtrack CWC application technical architecture is not up to the standard expected. An architectural review is on-going, once complete actions will be agreed with Transtrack's management to reduce the risk of future technical issues.	Rob Houghton	Description of risk around Transack is linked generically through to Risk Note as a part of risk to Technology and Business Interruption
			2	**Group Risk - GLO - Customer confidence in Horizon online system.** The case of the Horizon system is currently underway. The outcome of this case may impact the agents and clients confidence in using the system and risk reputational damage.Mitigation plans are being built in response	Rob Houghton	Description of risk around system confidence is linked through generically to Risk Note as a part of risk to litigation.
			3	**Computer Centre inability to perform automatic failover.** CC have advised that the current version of software which connects service for branch and admin users is currently out of date. In the extremely unlikely event of a major disaster CC are currently unable to perform automated failover from the primary datacentre to the secondary datacenter, the switch from primary to secondary would require a manual failover. This would result in the service being unavailable within branch and for admin users for period of time until manual failover is complete. Manual fall back processes and procedures are in place to restore service as quickly as possible and best efforts will be made but the service outage risks exceeding RTO. The upgrade of the software has been requested and this is expected to complete in 10 weeks.	Rob Houghton	Description of risk around Computer Centre failover is linked generically through to Risk Note as a part of risk to Technology and Business Interruption
THIRD PARTY	Contract Management	Material new contracts or extensions entered into, direct awards and where I have not followed the contract process	4	**Non-compliance with PCR.** There are a low number of contracts signed or extended which were not procured or extended in line with Public Procurement Regulations 2015. They are generally low risk and with a commercial imperative. New controls have been introduced to record incidents or exceptions going forward. This will bring greater clarity over level of non-compliance with PCR. All non compliant extensions and awards are logged and reported to the RCC on a quarterly basis.	Jane MacLeod	Description of risk around non-compliance with PCR is linked generically through to Risk Note as a part of risk to Legal and Regulatory Breach
LEGAL & REGULATORY	Managing losses and Fraud	Material frauds, irregularities or losses that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners	5	**Banking cash deposits.** Most issues relate to high value Santander Business Banking deposits but as the BFS expands, this is migrating. The annual training was significantly re-written this year to help branches to identify and report issues. A new procedure has also been implemented to identify and report large volumes of Scottish and Irish note deposits from locations remote from the Scottish and Irish borders as these are frequently indicators of criminal street cash laundering. There have been a number of investigations involving high value business cash deposits and, at the request of the MLRO, the Post Office Legal team are currently reviewing the MLR requirements for Post Office in relation to these transactions to ensure that there are no additional regulatory obligations on Post Office, and that customer due diligence and transaction monitoring remain the responsibility of the banks within the Banking Framework Services contract. Financial Crime and Legal are liaising with Pinsent Masons to establish the exact regulatory position/risks and also working with the Santander FIU (Financial Intelligence Unit) to raise our concerns about some of their customers activities.	Jane MacLeod	Description of risks around fraud are linked through generically to Risk Note as a part of risk to Legal and Regulatory Breach
FINANCIAL	Reporting results, providing data accurately and effective internal controls	Complex or subjective accounting judgements, estimates and revenue transactions	6	**GLO.** On 11 April 2016, a High Court claim was issued on behalf of a number of mostly former postmasters against Post Office in relation to various legal, technical and operational matters ("the **Post Office Group Litigation**"). Per POLs accounting policy for exceptional items and as agreed with EY, the expenditure associated with the Post Office Group Litigation should be accounted for as an exceptional item. Subject to Final Audit, the incurred costs for FY 2018/19 is £13.7m.	Jane MacLeod	**To be disclosed**
			7	**GLO – Reclaiming losses found on audit.** As a result of the Common Issues trial judgment our practices relating to the recovery of losses found at audit will need to change. Monies recovered during 2018/19 totaled £2.2m, but it is estimated this figure will reduce to c.£1m during 2019/2020.	Rob Houghton	Requiring accounting judgement
			8	**GLO – Payment of Remuneration during suspension.** As a result of the Common Issues trial judgment, Post Office is now continuing to pay full remuneration on suspension. This could lead to double costs to run Post Offices where a temporary Postmaster is installed for service reasons. A decision paper is currently being worked through to find a reasonable compromise where the remuneration amount paid to a suspended operator reflects their actual branch overheads; if a temporary Postmaster is paying the staff for example, this element would be deducted. Any approach will need to be legally assured in the context of the GLO judgment, but the current estimate of additional cost if not addressed is £2m.	Rob Houghton	Requiring accounting judgement
			9	**Assurance work has not been performed on Fujitsu.** At this point in time due to delays in Fujitsu providing rectified reporting. This work is scheduled to be performed in May/June. This is in light of the Telco accrued revenue error noted in FY17/18. The risk is that there could be errors within revenue that haven't been identified. However the FS&T team have obtained a revised report that they've assessed and PWC performed some specific work over the issue at the start of FY18/19 therefore the risk is partially mitigated.	Michael Passmore	Requiring accounting judgement
			10	**Changes to accounting policies:** - P&S stock provisioning – change in policy to better reflect stock usage/lifecycle - Branch cash fraud provision – review and slight amendment of methodology - Holiday pay accrual - review and slight amendment of methodology - Royal Mint Coin provision – change in provision policy based on expected sales forecast however provision calculations not reviewed in detail by group finance	Michael Passmore	Requiring accounting judgement
			11	**ATM cash holding.** Unquantified risk, but will be known prior to signing, within the ATM cash holding which has not been provided for as at the time of writing. Reporting capability of the system and historical data loading methods do not allow complete / sufficient analysis.	Michael Passmore	Requiring accounting judgement
			12	**Risk within Agency Billing** (unquantified): - Mapping of products/VAT settings/Archiving of data before invoicing/rounding issues – all of these are resolvable but carry a risk of delayed issue and/or non-payment of invoices - Customer Settlement process is now not working – there appears to be missing data - Only 2 people in have sufficient knowledge and understanding of the old and new billing methods, leaving a risk of being unable to issue invoices timely and correctly	Michael Passmore	Requiring accounting judgement
			13	**CWC impact post Back office Go-Live.** Ongoing issues with the CWC system have a continuing unquantified impact on the business including, but not limited to: - Incorrect reporting of the split of cash holdings and related balances - Potential under/over hedging of foreign currency holdings - Manual workarounds being required for a number of processes across the business - Increased cost base within supply chain to deal with the issues	Michael Passmore	Requiring accounting judgement
STRATEGY	Competitiveness, Market and Customer Relevance	Material risks to Post Office that are not captured in the Group Risk Profile	14	**Co-op Group and / regional Co-op Societies.** We believe this risk has been partially mitigated through improved stakeholder management with some of the individual Co-Operative societies coupled with a joint working approach with FRTS (the joint buying group for the Co-Operative Group) to complete detailed analysis of the deployment of the PO operating model in the Co-Op.	Debbie Smith	Description of risk around disengagement from Post Office by Co-Op Group (TCG) is linked through generically to Risk Note as a part of risk to Retail Proposition and Network Sustainability

5.1

POL00423567

Annual Report and Accounts 2018/19

Top Risks, Executive Declaration, and Risk Management Section for ARA

Author: Deana Herley Sponsor: Jenny Ellwood Meeting date: 09 May 2019

Executive Summary

Context

The purpose of this paper to review and agree the draft principal risk in the Annual Report and Accounts (ARA) 2018/19. Updates have been made following a review of the top risks and Executive Declaration results. The top risks is a summary based on feedback from all GE members and is a consolidated view across the Post Office business. The Executive Declaration process enables Group Executive (GE) members to consider (and attest annually) as a part of year-end procedures, if any additional disclosures are required to the principal risks to be included in our ARA.

Questions addressed in this report

- What is the current profile of our top risks in appendix 1?
- What are the outcomes of the Executive Declaration in appendix 2?
- Are the proposed Principal Risks as mapped in appendix 4 the correct risks for inclusion in the ARA?

Conclusion

1. We have performed a robust and systematic review of our risks that we believe could have a material impact on the results, condition and prospects of Post Office. The proposed principal risks set out in appendix 4 are those which will appear in the ARA and have been drafted based on the position of top risks (appendix 1) and are supported by the Executives' Declaration results (appendix 2). We show the alignment of items to our priorities.

Input Sought

The Committee is asked to review the information provided in appendices 1-4:

- Agree proposed changes to our top risks;
- Note the Executive Declaration outcomes;
- Confirm the approach to ARA disclosure as set out in this paper; and
- Consider whether there are any other matters that should be included and reported against.

POL00423567

The Report

What is the current profile of our top risks in appendix 1?

1. Since March RCC meeting, marginal changes have been made to the top risk profile (see appendix 1) which include the following:
   - We have 12 top risks. 1 risk has slightly increased relating to Technology and Business Interruption (Computer Centre automatic failover) has increased in impact (5-2 from 3-3) as a result of being unable to automatically failover to the 2nd datacentre. Manual failover is possible however, and as there have been few historic events which have led to a failure so probability reduced but impact increased. The likelihood of the Group Litigation risk has increased to a 3 (possible) from a 2 (unlikely), impact remains as a 5 (5:3). All other risks (10) have no changes to impact and probability scores.
   - Top risks considered as key are disclosed generically in the Risk Note section of the ARA, as summarised in appendix 4.

What are the outcomes of the Executive Declaration?

2. The Executive Declaration returns have been reviewed for materiality and consistency against Internal Audit and wider Business Assurance reviews, resulting in 16 items being disclosed with 14 items of materiality (29 items disclosed and 14 of materiality last year) being summarised in appendix 2 including:
   - 1 item of material significance that will be disclosed as a contingent liability re – Post Office Group Litigation.
   - 6 items are to be disclosed generically in the Risk Note section of the ARA.
   - Outputs (7 items) requiring an accounting judgement to determine the need for any adjustment have been reviewed by the Financial Controller.
   - 2 items were also considered by the GE owner, but were determined as being not material or sufficiently addressed by other generic disclosures.
3. There has been a direct correlation in the number of items reported with the maturity of our risk reporting processes (*Incident Reporting, Exceptions, Complaints, and Risk Registers – including identification and reporting*).

Are the proposed Principal Risks as mapped in appendix 4 the correct risks for inclusion in the ARA?

4. The proposed wording around the 'Management of Risk' which will be included in the ARA is set out in appendix 3 and principal risks (appendix 4) proposed for ARA inclusion and have been drafted based on the position of top risks (appendix 1) and are supported by the Executive Declaration outcomes (appendix 2). The arrows indicate risk movement.

POL00423567

Appendix 3: Management of Risk

Our Approach to Risk

The commercially competitive and highly regulated environment, together with operational complexity, exposes the Post Office to a number of risks. We define risk as anything that can adversely affect our ability to meet the Post Office's objectives, maintain its reputation and comply with regulatory standards. We seek to understand and harness risk in the pursuit of our objectives and aim to operate within an acceptable level of risk taking. The Post Office has articulated its risk appetite in relation to the most material risks with a view to managing better the key strategic risks and assessing the risks in relation to new opportunities.

Risk Management Governance

The Board is accountable for risk management and internal controls in the Post Office, reviewing their effectiveness and determining the nature and extent of principal risks. The Board has delegated responsibilities to the Audit, Risk & Compliance (ARC), which provides assurance to the Board through review of reports from management, risk, internal audit external advisers and external audit. Responsibility for day to day operations rests with the Group Executive (GE). The Risk and Compliance Committee reviews the effectiveness of the risk management framework and management of principal risks. It is chaired by the General Counsel, membership includes all of the GE and the output is reported to the ARC.

Our Risk Management Framework

In order to deliver its objectives, the Post Office is required to identify, assess and manage a wide range of risks. These are managed through an overarching framework in order to apply consistency and transparency of risk management across the organisation. The framework identifies roles and responsibilities of key parties in the risk management process, the policies for how risks are managed, the tools and processes used and the reporting outputs that are generated.

The approach to risk management is based on the underlying principle of line management accountability for effective implementation of internal controls to manage risk. The Group Executive has identified and manages the principal risks in the organisation, focusing on the aims of the strategic plan. These risks, with their response plans, are reviewed by the Central Risk team and at the Risk and Compliance Committee and the ARC to assure the robustness of risk assessment and management. There is an ongoing process of identifying, evaluating and managing the principal risks faced by Post Office.

During the year we have further improved our oversight over the level of risks being taken across Post Office and effectiveness of our mitigating actions, including close monitoring of emerging risk themes and incidents. Plans are also in place to fully refresh risk appetite to better inform decision making. This is a component within our wider enhancement plan to continue maturing our Risk Management framework.

Our Control Framework

We have an internal control framework in place for both our financial reporting and IT processes, which fall under our self-assessment regime. In addition, we have implemented a suite of Post Office policies which define the minimum control standards we expect to be performed within the applicable business areas. Our risk management efforts are also underpinned by our Executives' Declaration.

What's changed since last year?

[Section to be completed post agreement of Draft Principal Risks with risk movement]

POL00423567

Appendix 4: Proposed Principal Risk

Draft Principal Risks*	Movement	Top Risks	Executives Declaration
Strategic Risks			
Dependency on strategic relationships Post Office has a number of strategic relationships which are key to delivering its growth and strategic ambitions. The number of such relationships are increasing. We work with our partners to align our direction and interests to enable us to meet evolving customer and market requirements and any misalignment.	↓	[9] Sustainability of the Business Model	
Retail Proposition Post Office are committed to maintaining a Retail network of at least 11,500 branches. Critical to this objective is offering an attractive proposition for our retail partners and to continue to operate Post Offices in communities who need us. We continue to review and develop our proposition to enable us to continue to successfully deliver our social purpose, which addresses the impact of: • increased high street costs • ongoing move to online; and • a decline in traditional income streams.	↔	[2] Retail Proposition [6] Digital Competency [7] FS&T Market Development and Competition [9] Sustainability of the Business Model [3] PO Group Litigation	[14] Co-op Group risk (TCG)
Economic and Political Environment Current uncertainties in the external political, economic and social environment could have a detrimental impact our strategy and operating model significantly: **Brexit** itself represents a potential series of risks which would be most pronounced in the event of a no-deal departure from the EU (see below), but has also taken a very serious toll on all aspect of Government and politics more broadly. There is little room for meaningful Government activity in other areas, and splits in both main parties. There remains a possibility that the current impasse will increase the pressure for a General Election, with the attendant risk that Government and our Shareholder's priorities will change in favour of a Labour agenda, with significant implications for the business. Examples include the implementation of Labour's proposals for the renationalisation of RMG, and the creations of a Post Bank. **Brexit No Deal Implications:** - disruption to operations (customs labels in branch, accessibility issues for supply chain) - spending patterns of our customers during economic uncertainty and potential downturn of the economy e.g. decline in the sale of banking products, particularly mortgages - financial resilience of our postmasters and suppliers; - retention of skilled labour and recruitment	↑	[8] Appropriate actions for Brexit risks have not been considered	

Strictly Confidential

5.2

POL00423567

- new income streams failing to grow.			
Operational and Financial Risks			
Business change Performance, operating results and future growth is dependent on the Post Office's change programme. Expected benefits may not be achieved due to: • any change funding support; • savings delayed or not achieved; or • a decline in appetite for new change.	NEW	[2] Retail Proposition [6] Digital Competency [11] FS&T Regulation	
Health and Safety Due to Post Office's wide reach through the size and operation of its Network including fleet, our safety outcomes have occasionally had an unfavourable human impact. A health and safety incident or failure could result in serious injury, ill health or loss of life.	NEW	[12] Safety Compliance	
Technology and Information Security Risks			
Technology, Business Interruption and Cyber As the digitalisation of our business continues to grow, Post Office is dependent on the continued effectiveness, availability, integrity and security of its information systems and associated infrastructure. Post Office, in common with other businesses, is continuing to track the threat "universe" and is aware of increasing risk from cyber-attackers seeking to undermine businesses, government and utilities.	⟺	[10] Technology and Business Disruption [5] DR / BCP plans [4] Cyber Threat	[1] Transtrack [2] Computer Centre Failover
Legal and Regulatory Risks			
Group Litigation A group litigation being brought by a number of mostly former postmasters, alleging defects in the Horizon system and Post Office's internal processes. The resolution of these claims is now proceeding through the Courts (Bates & Others v Post Office Limited, High Court Justice (QBD) Claim No's HQ16X01238, HQ17X02637, HQ17X04248).	NEW	[3] PO Group Litigation	[3] Horizon
Regulatory Environment Post Office operates under an extensive and evolving regulatory environment, including areas such as financial services, transactional services, postal services, telecoms, procurement, competition law, and data security. This environment continues to evolve, particularly in the financial services (e.g. HMRC's requirements around Anti Money Laundering controls, location fees as well as Fit and Proper) and telecoms space, which increases the risk of non-compliance, costs and could impact our financial performance.	⟺	[1] PCIDSS [11] FS&T Regulation	[4] Non-compliance with PCR

5.2

*Potential Consequences and Key Mitigations will be drafted post RCC agreement.

POL00423567

Compliance Report

Author: Jonathan Hill Sponsor: Ben Foat Meeting date: 09 May 2019

Executive Summary

6.1

Context

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

Questions this paper addresses

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

Status Update

Sector	Current Assessment	Previous Assessment	Comment/Action
Telecoms Compliance			Ofcom has confirmed it is to investigate the Text Relay issue and we are supporting it with its information requests. We have signalled that we are open to exploring an early settlement, which was proposed by the regulator may be offered
Information Protection & Assurance			The data incidents previously reported have closed with little impact to Post Office. The DPO has returned to full time work following a long-term illness
AML/CTF			We have received confirmation from HMRC that branch registration fees are increasing from £130 to £300 per annum with effect from 1st May 19. This will have a significant impact on our annual renewal fees which are due on 1st June. HMRC has agreed our position on Officers in Charge and is comfortable with an extension up to beginning September for registering agents for fit and proper
Whistleblowing			No material issues to report. Analysis of February's Whistleblowing survey has been undertaken and we are now working with HR and a newly formed Ethic's Code of Business Task Force on how to promote the key messages and improve the service.
Anti-Bribery and Corruption			Starting in Q1, the Financial Crime team will monitor the Selenity expenses report quarterly and compare these against the quarterly Gifts & Hospitality report to identify any potential discrepancies
Supply Chain Compliance			14 improvement needs from 4 audits in the 3 months to April. No material issues - satisfactory overall
Financial Services Compliance and Conduct Risk			Within appetite overall, however, we are working with FS on strategic product change initiatives for credit card new providers and current account closure. This includes new Appointed Representative agreement and management of new regulatory Principal.
Vulnerable Customers			Alternative format literature provision-we are currently at the final stage of contract negotiation with an external provider. When complete this metric should move to green (expected end May)

POL00423567

KEY:

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

Commented [JEH1]:

6.1

Input Sought

The Committee is requested to note this paper

POL00423567

Report

Key issues

Telecoms Compliance

Text Relay

1 Ofcom has issued a draft Section 135 notice to support its investigation into the text relay issue. We are engaging with the regulator to ensure we meet its requests for information. Ofcom has recognised the actions we have already taken to fix the billing system for text relay calls, our commitment to reimbursing impacted customers and that we have self-reported, which is anticipated to help reduce any penalty the regulator may seek to impose

2 Ofcom has indicated that it may be prepared to enter into early settlement discussions, and we have responded saying that we would be interested to explore this approach.

3 We will be compensating customers. Fujitsu is producing the data extract to enable us to identify impacted customers.

Complaints

4 The customer complaints data for Q3 18/19 was published by Ofcom in mid-April and shows that Post Office continues to be under the industry average for both landline and broadband.

5 Also, Ofcom has published its Comparing Service Quality Report, which shows that Post Office has one of the shortest call waiting times in the industry. However, it has also indicated that Post Office landline customers have one of the most reasons to complain although this is based on data from December 2017 and does not reflect the improvement made. In the 12 months between Q4 2017 and Q4 2018, we have seen our Ofcom complaints for our Landline service drop by 62 per cent, down to below the industry average.

POL00423567

Information Protection & Assurance

Data Protection

6 At the end of December 2018 we were alerted by the National Cyber Security Centre (NCSC) to 50 Post Office accounts being available through an Iranian state exploit of multiple companies. All 50 accounts had very weak passwords and upon notification they were all promptly locked down and forced to use strong passwords. The NCSC have come back to Post Office, and it is satisfied that there was no evidence of a further hack. Additionally it is satisfied with the measures that we have taken to protect against a repeat event.

7 Also at the end February Verizon Cyber Risk Program advised Post Office that a collection of 29 billion stolen users' credentials (usernames and passwords) had been published in the Dark Web in January. From these stolen users' credentials there were 40 that appeared to be from the Post Office. The programme went out on Sky News highlighting the fact that Post Office (and other companies) were affected, there has been no noticeable increase in requests as a result.

Compliance

8 We are preparing for our next ISO27001 audit due in June, to be conducted by Lloyds Register. We do not anticipate any issues will be raised at this audit.[1]

Financial Crime

Compliance with Money Laundering Regulations

9 Between 25th February and 23rd April 2019, 68 new Bureau de Change non-conformance cases were identified. During the same period 81 open cases were resolved, of which 24 related to customers who had purchased in excess of €15k in 90 days, which breached the regulatory limit and mitigating actions have been taken.

10 At the beginning of April, the Data Centre of Excellence provided resource to resolve the outstanding issues with the Bureau de Change transaction monitoring system and to develop the additional reports that had been agreed with HMRC. Good progress has already been made with some minor issues rectified and some of the new reports built and tested.

Anti-Bribery and Corruption ("ABC") update

11 ABC training completion is at 98%. We continue to see some colleagues reporting gifts and hospitality via the reporting tool incorrectly and/or not conforming to policy and a further communication has been issued about not accepting cash. Starting in Q1 2019/20, the Financial Crime team will monitor the Selenity expenses report quarterly and compare these against

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

POL00423567

the quarterly Gifts & Hospitality report to identify any potential discrepancies.

Whistleblowing update

12 No material issues to report. Analysis of February's Whistleblowing survey has been undertaken and we are now working with HR and a newly formed Ethic's Code of Business Task Force on how to promote the key messages and improve the service.

Fit and Proper

13 The focus since the last update has remained on gathering full F&P returns:

14 The project team continue to work with each Commercial Partner, supported by the Account Management team and the number of full and complete returns is rising.

15 Likewise, for non-commercial partners, a Chesterfield team (13 FTE) has cleared a backlog of c.1000 responses and are focusing on outbound phone contact with Agents who have submitted partial responses, or raised queries. Network Area Managers are also providing support. Reminders have been sent to non-responders, although those now constitute a small proportion of the at-risk income, compared to the partial responses. Efforts remain prioritised on those Agents with the highest at-risk income.

16 MI on our data gathering progress is being collected weekly and shared regularly with HMRC. As a result, HMRC has agreed to an extension to September 2019 should we need it. However we are still working to achieve the June target.

17 Alongside the data gathering, a bulk revoke and reinstate solution for branches is in development. The technical solution will be supported by governance and processes will be in place to decide whether services will be revoked and how changes will be communicated (i.e. data supply to the correct stakeholders, communications to affected Agents and briefing to and preparation for impacted POL business areas - e.g. NBSC).

18 Even though progress with returns may support deferring the deadline for revoking branches' Travel Money capability, the project team is working to prepare the revoke and reinstate functionality and the supporting process model so that it is ready ahead of the June HMRC report production cycle.

19 We wrote to HMRC in March setting out our legal view in relation to the F&P requirements for Officers in Charge/Agent Branch Managers (a requirement that would have given rise to significant additional cost), and they responded in April that POL does not need to extend F&P requirements to OIC level, however, they have reserved the right to review the position regarding staff undertaking branch management roles as part of any future compliance activity and if they deem, in specific instances, they are within the scope of the relevant guidance, POL will need to submit their details as part of the agent list.

Regulatory updates

20 We have received confirmation from HMRC that branch registration fees are increasing from £130 to £300 per annum with effect from 1st May 19. This will have a significant impact on our annual renewal fees which are due on 1st June. Corporate Affairs has already reached out to BEIS and ongoing

POL00423567

discussions continue internally between the Legal and the Travel Money teams to consider whether we have a right to appeal and next steps.

21 HMT has published the consultation paper on the transposition of 5MLD into UK law. We have until the 10th June to respond and are engaging with stakeholders including the Travel Money team with regards to potential implications for Travel Money/MoneyGram and the Identity team with regards to electronic ID. The Legal team is also supporting this review to determine the potential wider implications for Post Office and how we will respond to the consultation.

External threats

22 A meeting was held with Santander MLRO to discuss the ongoing concerns with the continuing high levels of Financial Crime investigations predominately relating to business cash deposits. Santander advised that they are currently testing whether they can restrict the daily amount their customers can deposit over Post Office counter which should reduce the risk to POL.

Internal threats

23 Financial Crime risk assessments and re-assessments have been completed for 30 products and services. No major internal threats have been identified, and the outcomes have been shared with the Risk team to ensure that any risks are identified and reflected in functional RACMs. The Partner Banking Framework Services reassessment started at the beginning of April and we expect this work to be completed by the end of May.

Supply Chain Compliance

24 Four audits were completed in the three months to April. 14 Improvement Needs were identified, with a combined audit score of 28, averaging 3.5 Improvement Needs and an audit score of 7, which is fractionally higher than the rolling average for all Supply Chain sites keeping them in the Satisfactory category for both measures. No significant or recurring issues.

Financial Services

Notification of Approved Person

25 Following his appointment as Interim Chief Executive; Al Cameron has agreed to be the FCA Approved Person in respect of the Appointed Representative Function (CF 3 Chief Executive AR) for BoI and POMS. A briefing in respect of the duties and responsibilities of an Approved Person was provided by the Compliance team. The requisite notifications for approval will be made to the FCA via our two Principals who will also meet Al Cameron for separate briefing(s).

Credit Cards

26 We continue to work with our legal advisors, product teams and the new potential Principal on an Appointed Representative Agreement (ARA) with Cap One. This will also entail changes to the existing ARAs with BoI and POMS. As well as a new multi principal agreement (MPA) between all the Principals. The MPA is to ensure that boundaries of regulatory responsibility

POL00423567

are clear between Principals and are largely dividing responsibility along product lines.

27 Any new Principal agreement needs to be consistent with the approach taken with our existing regulatory Principals to ensure consistency of application and purpose. Following the agreement on the ARA we will need to put in place a Regulatory Guidance Manual with Cap One that outlines the key responsibilities PO has to put in place to maintain compliance.

Current Account withdrawal

28 The PO Money current account was withdrawn from sale in March and the existing 21,500 customers have been written to confirming that BoI is closing their account with closure aimed at 11th September 2019.

29 The communications plans for the withdrawal of sale of current account were agreed by the Compliance teams. All 39 branches offering current accounts received a personal visit from a senior manager to explain the change and Horizon screens were updated to effect the withdrawal. So far we are unaware of any spikes in complaints related to this closure but it is early days.

Mystery Shopping

30 Both Video Mystery Shopping for Customer Relationship Managers and Counter mystery shops (non-video) are trending within appetite.

Network management changes

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

Vulnerable Customers

32 A series of 'One' communications have been being issued to raise awareness and flag sources of external support. The graduates are working on a branch check list initiative working with the Alzheimer's Society to help provide guidance to make Post Offices more dementia friendly. This was presented together with the Alzheimer's Society at the NFSP Conference.

33 An external accessibility expert Kate Nash Associates is currently reviewing the PO Vulnerable Customer Policy for completeness. We also propose some independent work with her to gain an independent view on Post Office's vulnerability approach and how we can improve.

34 The launch plan for the digital Vulnerable Customer Module and test is being designed with the Training Team with the expected launch on 20th May. This will include communications and Team Talks for those that do not have access to Success Factors.

POL00423567

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

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

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

Telecoms/Broadband

37 Ofcom had already planned to introduce end of contract notifications and annual best tariff reminders for customers who are out of contract. At the same time of the CMA announcement in December, Ofcom also announced that it is reviewing the pricing differential. Ofcom has expressed concerns about vulnerable customers who are out of contract and being charged high prices, with a particular focus on over 65s. We met with Ofcom in February as part of our on-going relationship and expressed concerns. Ofcom agreed that it shouldn't use such a broad brush to define vulnerability.

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

Mortgages, Cash Savings & General Insurance

39 The has been one development in this area since the last report The FCA has issued new proposed rules to be in force by the end of 2019 on the mortgage prisoners challenge, (customers that are up to date with their mortgage payments but cannot re-mortgage because they would fail FCA rules on eligibility). We will work with BoI to assess approach/impact of new eligibility rules and any new opportunities these may present.

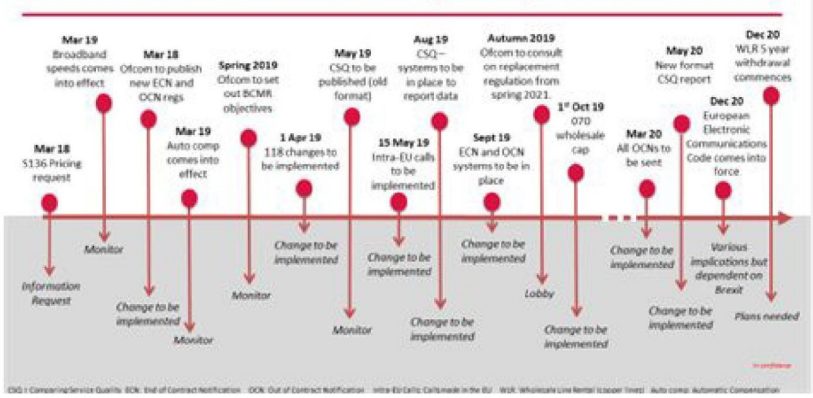
Jonathan Hill

Compliance Director
May 2019

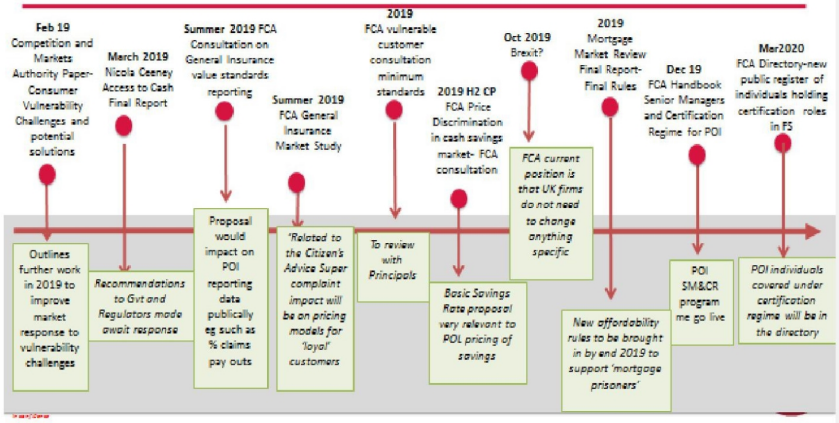
POL00423567

APPENDIX

Post Office Telecoms Regulatory Calendar



Post Office Financial Services Regulatory Calendar



9

POL00423567

Post Office Compliance - March 2019

Risk ratings

March risk ratings and how they compared to February

Press For Descriptions

TELCO	Customer Satisfaction	◄►
	Customer complaints sent to ADR	▼
	HP/BB % Of Branches Trained	◄►
FINANCIAL SERVICES	Overall Mystery shops rated Red	◄►
	Miss Selling Upheld Complaints BoI	◄►
	Customer Complaints POI	◄►
	Life Cancellations	◄►
	Travel Ins Cancellations	◄►
	Financial Services Number Of Branches Trained	◄►
	Insurance Number Of Branches Trained	▲
IPA	Data Protection Incidents	▲
	Supplier Management	▲
	IS & DP % of Branches trained	▲
Financial Crime	Bureau - customer transaction limit breaches	▲
	Supply Chain Audit Issues	◄►
	ABC % of Branches trained	◄►
	AML % of Branches trained	◄►

Risk ring and overall performance rating: **Amber**

Based on the weighted cumulative outcome of the KRIs we measured in March, the overall risk rating is Amber.

Green rated KRIs	Amber rated KRIs	Red rated KRIs
13	3	1

This month we were within tolerance for 16 out of the 17 KRIs we measured. 13 of our KRIs were rated green and 3 of our KRIs were rated amber. One of our KRIs was rated red. In comparison, in February we exceeded tolerance in 4 of our KRIs and in March we exceeded one of our tolerances.

Distribution of KRI risk ratings between April 2018 and March 2019

Exceptions and key trends

Telco Customer Satisfaction still positive. Slight decrease was due to an issue in the Talk Talk network for Safeguard Parental Controls. This has now been fixed.
Work has been going on to improve our signposting to Alternative Dispute Resolution which may cause more complaints to go to the Ombudsman however this should reduce over time as improvement are also made to ensure these are resolved at an earlier stage. The Homephone and Broadband workbook is due to be completed during the period 22/3/19 - 16/4/19. 60% of colleagues have completed the training to date.

Video Mystery shops - Performance had improved greatly in January and February however March has seen a slight increase in Reds for Savings at 15%. 2 Red VMS in March, one as a result of the summary box leaflet not being given to the customer the other was due to advice being given. Red rated Insurance shops have improved, performance for March is 5%, and is the first month where the Life Insurance results have dropped below 10%. Branch Mystery shops - 67 Savings shops were completed in March, of these 3% were graded Red which is within our tolerance levels. 123 Insurance mystery shops were completed in March, of these 19% were graded Red which is above our tolerance levels. No upheld branch mis-selling complaints for BoI products or for POI products were recorded. The highest rate for cancelltion of Over 50s policies is from applcations completed via telephone to the call centre at 6.1%.
Financial Services workbook was completed during the period 7/1/19 - 30/1/19. 97% of branches have completed the training. Insurance workbook was completed during the period 15/2/19 - 11/3/19. 98% of Branches have completed the training.

Supplier Management - the pilot to improve supplier capabilities during a cyber incident has been successful. An expansion plan to include more of our critical suppliers is underway. Examples of some of the issues we are focussing on: Accenture - have missing DR in place for some systems. Atos - missing patches for the call logging system, and non-obfuscated data held in test systems. ComputaCenter - not all servers have Antivirus running (Linux), the log analysis software has failed, thus no review of security logs can occur reliably, and they have not concluded their data mapping task. Verizon - have highlighted an issue with DXC access to Post Office systems - this is a terminating service, and Verizon are watching the activity closely.IS&DP Training - The new training modules for 19/20 are under development for release in June 2019. The figures will dip in June, until all colleagues have completed the new module.

18 breaches of the £10k over 90 day Bureau threshold identified against customers transacting for business purposes (Post Office's Bureau de Change is designed to provide low value travel money services and does not have the framework to faciliate business tranactions). All branches were contacted to provide education and SARs raised by the FCT.

4 pre-order transactions prevented avoiding potential breaches to the €15k (£13.5k) regulatory limit. The total value of funds prevented equals £33k. SARs were raised on all pre-order customers.
One audit completed during March in Glasgow identifying 5 improvement needs with a score of 7 on the ACS element. (this is an improvement on 6 improvement needs with a score of 16 identified last year).

1 High risk item on the NCS element of the audit requiring both Treasury and Supply Chain to ensure consistency and full alignment on the handling of Clydesdale backing assets.
45 employees non-compliant due to incompletion of ABC Training vs 59 in February (2 employees currently outstanding within LRG). At the end of February, 10 branches Bureau services remained off due to non-completion of the AML/CTF training. By March, all branches completed their training and had their Bureau services reinstated.

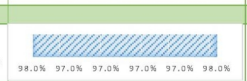
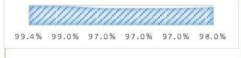
POL00423567

Key Risk Indicators

	How we measure Compliance	Risk Rating	Risk tolerance	In each of the last months: Sep-18	Oct-18	Nov-18	Dec-18	Jan-19	Feb-19	Measured in Current Month - March 2019	Key facts And Trends	Actions
TELCO	Customer Satisfaction											
	Levels of customer satisfaction give an indication about how likely customers are to complain to the regulator and how the regulator will feel about our general performance as regulations are in place to protect customers. Bad compliance normally results in unhappy customer		78%+ Green 72% to 77% - Amber 71% below – Red	79%	77%	77%	77%	79%	82%	80%	Telco Customer Satisfaction still positive. Slight decrease was due to an issue in the Talk Talk network for Safeguard Parental Controls. This has now been fixed.	RCA being conducted on Safeguard issue to identify learnings and prevent similar events occuring.
	Customer complaints sent to ADR											
	There are several metrics for complaints which we monitor. One of those metrics is reviewing how many complaints go to the Ombudsman as an ADR as we have either not resolved the complaint in 8 weeks or we cannot reach a resolution and have issued the customer with a deadlock letter.		10 or below - Green 10 to 20 - Amber	67%	100%	75%	3	7	11	11	Work has been going on to improve our signposting to Alternative Dispute Resolution which may cause more complaints to go to the Ombudsman however this should reduce over time as improvement are also made to ensure these are resolved at an earlier stage.	
	HP/BB % of Branches trained											
	Training of staff is a key control for Post Office in meeting our statutory and regulatory responsibilities. A minimum control standard in our Policies is that all staff complete training within 30 days of joining and annually. Tolerance level is set at 95% to reflect joiners and		No less than 95%	83%	83%	83%	83%	83%	83%	73%	The Homephone and Broadband workbook is due to be completed during the period 22/3/19 - 16/4/19. 60% of colleagues have completed the training to date.	
FINANCIAL SERVICES	Video Mystery Shops Rated RED BoI											
	The proportion of Agency CRM mystery shops for Savings rated red on a monthly basis.		No more than 10%	33.3%	0.0%	14.3%	16.0%	10.0%	8.0%	15%	Video Mystery shops - Performance had improved greatly in January and February however March has seen a slight increase in Reds for Savings at 15%. 2 Red VMS in March, one as a result of the summary box leaflet not being given to the customer the other was due to advice being given	Results continue to be reviewed and feedback provided to CRMs and ASPMS to help improvement.
	Video Mystery Shops Rated RED POMS											
	The proportion of Agency CRM mystery shops rated red for Life Insurance on a monthly basis		No more than 10%	13.5%	20.0%	19.4%	22.2%	18.2%	15.4%	5%	Red rated Insurance shops have improved, performance for March is 5%, and is the first month where the Life Insurance results have dropped below 10%.	Results continue to be reviewed and feedback provided to CRMs and ASPMS to help improvement.
	Counter Colleague Shops BOI											
	The proportion of Counter colleague mystery shops rated red on a monthly basis		No more than 10%	8.9%	5.0%	5.0%	0.0%	7.1%	9.0%	3%	Branch Mystery shops - 67 Savings shops were completed in March, of these 3% were graded Red which is within our tolerance levels.	Results continue to be reviewed and feedback provided to CRMs and ASPMS to help improvement.
	Counter Colleague Shops POMS											
	The proportion of branch mystery shops for Over 50s and Travel Insurance rated red on a monthly basis.		No more than 10%	22.0%	19.0%	17.5%	0.0%	21.5%	17.0%	19%	123 Insurance mystery shops were completed in March, of these 19% were graded Red which is above our tolerance levels.	A deterioration in the number of reds was identified, in particular colleagues not informing the customer of all products available in the Life Ins range. For Travel Ins the customer was not made aware of all 3 cover options. Several branches received retraining on TI last month. Fs Risk continue to monitor progress.
	Mis Selling Upheld Complaints BoI											
	The number of upheld branch mis-selling complaints per 100 products sold		No more than 1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0%	No upheld branch mis-selling complaints for BoI products	
	Customer Complaints POI											
	Total branch net sales vs branch distribution complaints received in the month		No more than 1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0%	or for POI products were recorded.	
	Over 50s life cancellations											
	The percentage of Over 50s sales cancelled within the 30 day cooling off period		No more than 10%	0.0%	12.0%	7.5%	9.0%	8.5%	7.6%	4.7%	The highest rate for cancellrion of Over 50s policies is from applcations completed via telephone to the call centre at 6.1%.	
	Life Cancellations											
	The percentage of Life Insurance sales cancelled within the 30 day cooling off period		No more than 10%	7.6%	0.6%	12.0%	14.0%	4.8%	6.0%	3.8%		
	Travel Ins Cancellations											
	The percentage of Travel Insurance sales cancelled within the 14 day cooling off period		No more than 2%	1.4%	1.7%	2.4%	2.4%	2.0%	1.5%	1.5%		
	Financial Services number of Branches trained											
	The number of branches who have completed the annual Financial Services regulatory workbook and test.		No less than 95%	100%	100%	100%	100%	95%	97%	97%	Financial Services workbook was completed during the period 7/1/19 - 30/1/19. 97% of branches have completed the training.	
	Insurance workbook number of Branches trained											
	The number of branches who have completed the annual Financial Services regulatory workbook and test.		No less than 95%							98%	Insurance workbook was completed during the period 15/2/19 - 11/3/19. 98% of Branches have completed the training.	
IPA	DP Incidents											
	Number of DP incidents		No more than 3	0.0%	6	57	47	44	50	1		
	Supplier Management											
	The number of late actions, deemed as critical by Post Office that suppliers have failed to resolve.		TBC							7	Supplier Management - the pilot to improve supplier capabilities during a cyber incident has been successful. An expansion plan to include more of our critical suppliers is underway. Exemples of some of the issues we are focussing on: **Accenture** - have missing DR in place for some systems. **Atos** - missing patches for the call logging system, and non-obfuscated data held in test systems. **ComputaCenter** - not all servers have Antivirus running (Linux), the log analysis software has failed, thus no review of security logs can occur reliably, and they have not concluded their data mapping task. **Verizon** - have highlighted an issue with DXC access to Post Office systems - this is a terminating service, and Verizon are watching the activity closely.	Each supplier has allocated action owners, and is committed to quick resolution.
	IS & DP % of Branches trained											
	The number of colleagues who have completed the annual regulatory workbook and test. Weighted average between support and branch figures		No less than 95%	93.0%	93.0%	93.0%	93.0%	93.0%	97.0%	98%	IS&DP Training - The new training modules for 19/20 are under development for release in June 2019. The figures will dip in June, until all colleagues have completed the new module.	New training modules currently under development
	Bureau - customer transaction limit breaches											

6.2

POL00423567

FINANCIAL CRIME	This is the number of customers that have: - Breached the £10k in 90 day limit by processing multiple transactions below the eKYC, PEP and Sanction threshold therefore circumventing internal limits - Material breaches over £20k that present genuine concern		0		0	18 breaches of the £10k over 90 day Bureau threshold identified against customers transacting for business purposes (Post Office's Bureau de Change is designed to provide low value travel money services and does not have the framework to facilitate business tranactions). All branches were contacted to provide education and SARs raised by the FCT. 4 pre-order transactions prevented avoiding potential breaches to the €15k (£13.5k) regulatory limit. The total value of funds prevented equals £33k. SARs were raised on all pre-order customers.	Monitoring to identify transactions under eKYC/ID thresholds is not currently being completed. FCT have enlisted the support of a Business Objects specialist to develop the monitoring reports. Monitoring due to start June/July.
	Supply Chain Audit Issues						
	Measure of effectiveness of supply chain compliance with industry regulation. ACS and ISO accreditation are required to maintain our cash supply and retain our NCS status		More than 24 red, 15-23 amber, below is green		6	One audit completed during March in Glasgow identifying 5 improvement needs with a score of 7 on the ACS element. (this is an improvement on 6 improvement needs with a score of 16 identified last year).	Timescales put in place with Glasgow to remedy the agreed improvement needs. Follow up meeting Mark Dixon sheduled to discuss the high risk item.
	ABC % of Branches trained						
	The number of colleagues who have completed the annual regulatory workbook		No less than 95%		98%	45 employees non-compliant due to incompletion of ABC Training vs 59 in February (2 employees currently outstanding within LRG).	Remaining employees are being chased via HR.
	AML % of Branches trained						
	The number of colleagues who have completed the annual regulatory workbook and test.		No less than 95%		100%	At the end of February, 10 branches Bureau services remained off due to non-completion of the AML/CTF training. By March, all branches completed their training and had their Bureau services reinstated.	

6.2

POL00423567

Cyber Security Update

Author: David Meldum Sponsor: Rob Houghton Meeting date: 9 May 2019

Executive Summary

Context

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

Questions this paper addresses

- What progress have we made on implementing the Security strategy?
- What is the progress of the implementation of Archer?
- What further remedial activities have we carried out as a result of the security incidents at the start of the year?
- What vulnerabilities were discovered during the penetration testing of the Payzone environment?

7.1

Conclusion

1. Funding for the initial transformation work for Security Strategy business case has been approved and a Programme Manager has been recruited to drive the delivery of the IT Security Transformation Programme. We continue to make progress around the identified 3 key areas – improving the reach and capability of the SOC, improving the management around Data Security; and improving the management and assurance of compliance of our 3rd parties.
2. Agreement has been made with the Risk function that RSA Archer should be the Governance Risk and Compliance (GRC) tool for Post Office and the rollout of the additional risk modules including third party assurance and top-down risk will commence in May.
3. The Cyber Security Incident Response Team (CSIRT) capability has been created to minimise the impact of security incidents by identifying the approach for preparing, identifying, containing, eradicating and recovering from security incidents. We have reduced the risk from Post Office colleagues utilising weak passwords by implementing a Microsoft Password Strength tool to force users to use more complex passwords.
4. IRM identified a total of 119 vulnerabilities including 5 that were critical and 28 assessed as high. A risk treatment plan has been created and remediation progress has been made for the identified weaknesses.

Input Sought

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

POL00423567

Report

What progress have we made on implementing the Security strategy?

1. The funding for the business case for the initial Security Transformation Programme was approved by CAG permitting the team to progress with the following activities:
    a. Improving the coverage and capability of the new security operations centre (SOC). Workshops have been held with Payzone, Post Office Insurance, Accenture CDP, Branch Hub and Fujitsu to plan and design the ingestion of their security logs. These areas will be on-boarded over the coming months increasing the visibility for the Security team across the Post Office estate.
    b. Improving our data security protection, which is protecting our data from leakage through people, processes, and technology/tooling. Workshops have been held with Post Office, Computacenter and vendors such as Microsoft and Symantec to design the use cases for data discovery classification, and prevention of loss in order for Post Office to select the vendor(s) that meet with their requirements. The final selection will be made in May and the commencement of the implementation of the solutions. A Data Analyst is being recruited to effectively manage the data that is discovered ensuring the relevant business owners are identified in order to validate the classification and access permissions.
    c. Improving the governance and assurance of our IT security posture over our 3rd parties to ensure they are not exposing POL to a possible breach. Whilst we have commenced regular Security reviews with our major suppliers to assure they are governing themselves we will now be implementing the RSA Archer Third-Party Risk modules in May to improve the overall visibility of our Third-Party vendor risks. We have recently implemented Recorded Futures as our Threat Intelligence partner which provide additional Third-Party Risk scores that can be used within RSA Archer.
2. A Programme Manager with a comprehensive track record in Transformation, Change Operations and Strategy has been recruited to drive the implementation of the Security Strategy. They will work with the Post Office Security Project Manager and the Third-Party Supplier teams to ensure the delivery of all aspects of the Security Strategy through the IT Security Transformation Programme.
3. The Deloitte maturity assessment of Post Office cyber security capabilities confirmed progress had been made in the first 3 months of 2019. Actions to address 76% of the capabilities, where a maturity shortfall was identified, are already in progress or have been included within the IT Security Transformation Programme. The additional 24% of the capabilities are covered by other areas of the business.
4. The following table shows the progress that has been made with the various Security Strategy initiatives:

POL00423567

Initiative	Time Line	Status	Outcome
Recruitment of CISO	January –May 2019	Completed	Recruitment of Group CISO to provide added focus on end to end security activity
Recruitment of Programme Manager	April 2019	Completed	Recruitment of Programme Manager to drive the IT Security Transformation Programme
Multi-factor authentication	November 2018	Completed	Ensuring all remote login's to Post Office environment requires a multi-factor authentication code
Security Operations Centre Go-Live	November 2018	Completed	Centralised security management into joint Verizon / Post Office Security Operations Centre
Recruitment of SOC Lead	January 2019	Completed	Recruitment of Post Office SOC Lead to drive continual improvement
Creating Post Office CSIRT	March 2019	Completed	Cyber Security Incident Response Team to manage security incidents and issues
Password Audits	December 2018 – March 2019	Completed	Proactive cracking of Post Office password directory to identify scale of issue with weak internal passwords
Disabled all users with weak Passwords	December 2018- April 2019	Completed	Disabling all users found to have a weak password. Being reviewed on a weekly basis.
Password Strength Tool Deployment	Go Live March 2019	Completed	Subsequent deployment of password strength tool, enforcing use of strong passwords
Microsoft Advanced Threat Analytics	Commenced February 2019	Inflight	Security insight on employee office 365 security – multiple logins in different locations, login whilst on leave etc
Threat Intelligence Platform	April 2019	Completed	Replaced Digital Shadows with Recorded Futures for an improved Threat Intelligence
zScalar SSL Interception	June 2019	Inflight	Interception of Encrypted traffic to determine if Post Office data is being removed from the environment
Data Discovery Phase 1	February 2019	Completed	Proactive scan of our active directory and share point environment to identify scale of unstructured data
Data Discovery Phase 2	April 2019	Inflight	Wider scan and auto-classification of data based on the results of Phase 1
Proactive Phishing Campaigns	February 2019	Continuous	Measuring the susceptibility of Post Office user base to simple phishing campaign
Red Teaming exercise	October 2018	Completed	Proactive Ethical hacking exercise simulating internet-based attack of Post Office
Deloitte Audit	January onwards	Completed/Ongoing	End-End Security assessment against industry standards and reviewing progress made in 2016 Deloitte Audit
Symantec Endpoint Protection Upgrade	Commenced February 2019	Inflight/Complete End of May 2019	Improving and updating the anti-virus and laptop protection suite for Post Office end users
Culture and Communications	January 2019	Ongoing	Regular messaging from Post Office leadership highlighting expectations around key security themes
Data Security Transformation Programme	December 2019	Inflight	Launched to deliver holistic data classification, protection and management
Third-party governance commenced	January 2019	Ongoing	Measuring and managing the compliance of our 3rd parties to internal security policies and standards
Security Enterprise Risk Management	February 2019	Completed	Quantifying and managing residual risk to report to ARC
Data Loss Prevention Suite (DLP)	Commenced April 2019	Business Case Approved/Inflight	To automatically prevent the egress of confidential or sensitive data from Post Office
Data Classification Tool	Commenced April 2019	Business Case Approved/Inflight	Users will be forced to security classify documents before they can save/print – enabling the DLP tooling
Security Operations Centre Enhancement	Commenced April 2019	Business Case Approved/Inflight	Ensuring full coverage of all critical systems and services in the SOC
Archer Risk Management Platform	Commenced April 2019	Business Case Approved/Inflight	Expanding the current use of Archer within the SOC into wider security management like 3rd Party assurance

POL00423567

What is the progress of the implementation of Archer?

5. The Security Operations Centre (SOC) Analysts continue to use the platform for managing security incidents that are raised from the Post Office SIEM (Security Information and Event Management) tool. Discussions have started with the Service Now team on the possibilities of integrating Archer with Service Now for Incident Management.

6. Discussions and workshops have been held between the Risk function, IT Security and RSA Archer. An agreement has been reached that Archer will be rolled out for Governance, Risk and Compliance (GRC) and all the commercials have been signed-off. We will commence the implementation of the third party assurance, security controls assurance and top-down risk modules in May 2019.

What further remedial activities have we carried out as a result of the security incidents at the start of the year?

7. Building upon the Security Operations Centre (SOC) we have created the CSIRT (Cyber Security Incident Response Team) Plan ensuring Post Office is prepared to react and manage Cyber Security incidents in effective and efficient manner. This will be tested regularly both internally and with suppliers to ensure all areas responsible for Security at Post Office are fully prepared to respond to incidents.

8. At the end of December 2018 we were alerted to 50 PO accounts being available through an Iranian state exploit of multiple companies by the National Cyber Security Centre (NCSC). All 50 accounts had weak passwords and as users continue to be our greatest threat we have now implemented the Microsoft Password Strength tool which checks the strength of a users' password and blocks them from changing it to a weak one.

9. NCSC have completed investigations on the Post Office cyber-attack in December and did not find any evidence to indicate any further breaches and are satisfied with the remedial actions that Post Office have implemented to prevent similar attacks in the future. The NCSC have also agreed to Post Office's revised legal consent letter with regards to future data exchanges which will permit a quicker engagement and support from the NCSC if necessary.

10. We have implemented the services of Recorded Futures as a Threat Intelligence platform that has replaced Digital Shadows. Recorded future uses machine learning and natural language processing to enable it to perform automated collection and processing of data at massive scale enabling them to provide alerts in matter of minutes rather than days. They also provide real-time contextualized intelligence highlights on our third parties alerting when they have vulnerabilities or actively under attack which in turn could affect Post Office.

What vulnerabilities were discovered during the penetration testing of the Payzone environment?

11. IRM were contracted to perform a penetration test of the Payzone environment to identify security vulnerabilities that could pose a risk to the business and included the following areas:
    a. Internal Infrastructure
    b. External Infrastructure

POL00423567

c. Branch devices
d. Android tablets and applications
e. Network Device Configuration
f. Build Reviews

12. The penetration tests identified a total of 119 vulnerabilities where 5 were identified as critical and 28 as high. These vulnerabilities could allow a threat actor to fully compromise the internal network and its data. It was also possible to leverage weaknesses within the application and mobile devices to obtain services such as top-ups without paying. IRM identified that these vulnerabilities were caused by a lack of due care for security, including unsupported or unpatched operating systems and poor internal security practices such as inherently weak passwords. Furthermore, the applications and devices reviewed were not designed to be resilient to attack, allowing a malicious user to tamper with the application and compromise devices.

13. Payzone has worked with Post Office IT Security department and the Information Security Risk team to formalise a risk treatment plan to remediate the vulnerabilities. Progress has been made where 1 critical and 14 highs have been closed.

Priority	Baseline	12/04/2019	26/04/2019
Critical	5	4	4
High	28	17	14
Medium	62	53	52
Low	24	24	24
Total	119	98	94

14. Payzone now have a fully patched server estate, with the exception of the unsupported machines which are subject to the replacement project. They have implemented a patch process to ensure they remain up to date with patching the environment. The remaining critical issues relate to systems where projects are staffed and underway with progress going to plan. Enhanced monitoring remains in place on all systems with no alerts triggered. Payzone continue to treat the remediation with the highest priority and will continue to work with Post Office Security teams to ensure the risks are reduced.

POL00423567

Resilience, Business Continuity & Crisis Management update

Author: Tim Armit Sponsor: Rob Houghton Meeting date: 9 May 2019

Executive Summary

Context

Operational Business Continuity is in place across key areas which meets business requirements. The 2018 audit report of business continuity capability identified gaps in the documentation and governance which needed to be addressed. This paper reports on progress against the audit findings and the current resilience and continuity position across Post Office.

There is a need to sign off the Business Continuity Policy annually which is due now.

8.1

Risks this paper addresses

- What is the status of resilience across Post Office and progress against the business continuity audit report.
- Annual sign off of the Business Continuity Policy.

Input Sought

The Committee is requested to sign the policy and note the report.

Conclusion

1. Audit responses are on schedule. This report focusses on responses for December 2018, earlier responses were reported to RCC and ARC on time in 2018.
2. This report covers the Risk Appetite for Business Continuity across Post Office and the Strategies adopted for resilience and business continuity.

POL00423567

The Report

What is the status of progress against the audit report findings due in December2018?

- The audit report found:

  Lack of strategic plan and consideration of risk appetite for BCM.

  The BC policy sets out Post Office's risk appetite; the strategic plan will be addressed by completion of the activities referred to in the risk appetite.

- A report is attached to this summary which details the appetite for all key areas where continuity and resilience solutions are implemented across Post Office. This focusses on :

  - Locations
  - Systems
  - Business Functions
  - Suppliers

- The document has been created following interviews and reviews across all areas. It has been validated by key business areas and there is some work ongoing.
- IT have their own controls in place for Disaster Recovery of systems and their own compliance measures. The appetite shown in the Business Continuity document is that of the business to the loss of systems.
- Contractual requirements are key in confirming the appetites ensuring Post Office recovery requirement meet contractual agreements. This review is ongoing across all business areas.
- The report below presents the appetite for all areas and the current situation for each area and how confident Post Office should be that the strategy in place meets the appetites requirements.
- From the report a plan will now be developed that allocates owners and people to action to reduce the level of exposure from unknown or red.
- The report will continue to grow as more business functions and suppliers are brought on board and as levels of resilience improve thus reducing the exposure.

What is the status of resilience and business continuity across Post Office?

1. Background - In 2016 Post Office had no planned recovery capability for its key locations or operations. It had a dysfunctional response to crisis and escalation with no clear reporting lines. There were no documented impacts of a failure and no plans per business area to be used in an incident. The historic Royal Mail group documentation in place across Supply Chain had become unfit for purpose. Controlled and manageable communication to staff and branches had not been possible.
2. Current position – The table below show the current status across Post Office with regards to crisis communication and business continuity capability.

   It is key that all staff can be communicated with in and out of working hours and that we can track staff safety in an evacuation. Post Office now has that capability in key offices and operations.

POL00423567

Post Office has never had the capability to simply communicate to all branches in the event of a Horizon failure and a solution for this has now been implemented.

Business continuity recovery strategies are now in place and tested for all location incidents.

3. Communication Status

Area	Capability	Status
Finsbury Dials	650 people via Grapevine single text blast	Tested
Chesterfield	350 people via Grapevine single text blast	Tested
Business Protection Team	all areas via Grapevine single test blast	Tested
GE Gold Team	all areas via Grapevine single test blast	Tested
Supply Chain	all depots, cash centres and trucks via Grapevine single text blast	Tested
Branches	every branch via Grapevine single text blast	Tested

4. Business Continuity Status

Location	Plans	Impacts	Strategy	Status
Finsbury Dials	In place	Known	Work from home	Tested
Chesterfield	In place	Known	Sungard Site	Tested
Bolton	In place	Known	Sungard Site	Tested
Bristol	In place	Known	Sungard Site	Tested
Supply Chain	In place	Known	Mutual Support	BAU
Swindon	In place	Known	Swansea	IT tested
IT systems	In place	Known	DR solutions	Partially tested

- Resilience in building design is being improved across key locations and resilience in contracts and IT is under constant review.
- Business Continuity is now established, embedded and moving from a development and implementation stage to a business as usual state that can be easily maintained and monitored. This changes the status of the role going forward.
- Future Challenges –The scope of business continuity covers all risks that may impact the reputation, income, customer service and operational capability of Post Office. As such all risks must be robustly challenged to ensure management have considered them and have responses in hand should they unfold. Areas being challenged:

POL00423567

a. Horizon failure across all branches for an extended period
b. Brexit
c. Political changes to Post Office and its operations including its role as a bank
d. Succession planning and key role risks
e. On-boarding new companies and roles of directors
f. Horizon trial and contingency responses
g. Risks of success across business functions
h. Cyber risks and the changes as we go forward

POL00423567

Business Continuity Risk Appetite

The report is divided into four sections:

1. An overview of the approach, the terms used and the assumptions that were used.

2. The risk appetite for key areas currently included within the business continuity programme.

3. Areas and risks which are not currently at a level that meets the desired risk appetite and a work status of the current strategies in place and assesses the adequacy of these to meet the desired appetite. This enables the reader to focus on only the key risks to Post Office.

4. Areas and risks which currently meet the desired risk appetite and presents how this is achieved and any further work that is required to continually improve this.

Assumptions:

1. A systems analysis review was completed across the business and IT in 2017 which identified the key IT systems and the required recovery times the business needed for these. This report identified Horizon and the networks as the only critical system within Post Office at that time. The impact of all other systems being down can be mitigated for two days with minimal affect.

2. The report focusses on business operations and appetite is considered from this standpoint. The business continuity and resilience team focusses on maintaining business services as such all assumptions are with this in mind.

Appetite Summary

The over arching simplistic assumption on risk appetite that underpins business continuity is that if the branches are open and the customers are being served then Post Office is operational. All other services which underpin the business and keep it functioning are seen as secondary if the primary objective is achieved.

The table below details the risk appetite for each key aspect of Post Office operations. The scope covers all aspects of Post Office for which continuity solutions are considered and will be updated and amended as the scope changes.

POL00423567

Areas within the report (the lists within these tables will continue to grow as more detail is gleaned during the work programmes):

Locations	Key locations which support Post Office operations directly. Most are within the direct control of Post Office some are covered by contracts. The dependency on the location and the resilience in design and recovery capability in place are all considered.
Systems	Key IT systems which support business operations are considered in terms of their significance and the disaster recovery solutiuons in place.
Business Functions	Key business functions which deliver or support Post Office operations.
Suppliers	External suppliers which deliver key services to support Post Office operations.

Risk Appetite is measured as:

Appetite	Impact and Tolerance	Requirement
Averse	Post Office has a low level of tolerance to any impact or outage. A solution to maintain the service is required.	1 day recovery or less
Neutral	Post Office can tolerate some downtime and the outage has tolerable impact. A solution is required but a longer period to recover is acceptable.	2 to 4 days recovery
Tolerant	Post Office can tolerate the service being non operational for an extended period of time with minimal impact.	Over 4 day's recovery.

Strategy Status is measured as:

Summary	Definition
Green	A solution is in place, it has been tested and meets business needs.
Amber	A solution has been identified that meets business needs but has not been tested.
Red	No solution is in place

POL00423567

Business Continuity Risk Appetite Off-Risk Programme - Red

The table below details the risk appetite for each key aspect of Post Office operations which do not have resilience or continuity solutions in place that would meet business needs in a crisis. The scope covers all aspects of Post Office for which continuity solutions are considered and will be updated and amended as the scope changes. This report is a live document and is ongoing as work is completed in areas and as areas are strengthened with solutions implemented and tested.

Risk Appetite Tables

Locations	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
POMS Glasgow	Averse	Loss of Insurance call centre support	Recovery Office	TBC working with POI on this.	Green
Preston Call Centre	Averse	Loss of POCA call centre support	Recovery Office	TBC working with the POCA team on this.	TBC
Fujitsu Belfast	Averse	Loss of Key critical IT systems including Horizon, POLSAP, MDM, Credence	Resilient design with zero down time and disaster recovery solutions	Full datacentre test has not been carried out for five years. Secondary datacentre is within the same region. Horizon branch data base has been successfully recovered in an alternative datacentre. Component tests of systems have been carried out successfully. MDM and Credence have been switched to an alternate site. Site is an N+1 site. Moving some to the Cloud which will improve resilience but not change contractual recovery times. Work to be done with IT to confirm each Data Centre has resilience in its design (infrastructure, power etc). The exit from Belfast will improve the levels resilience levels.	Red
Payzone Offices	Averse	Loss of Call Centre and head office functions	Recovery Office	Agreement to share old Payzone offices for a period of time. Planning in place to implement a Sungard solution to meet business needs and to increase the operational resilience within the office.	Red
Payzone Data Centres	Averse	Loss of Payzone operations	Resilient design across two data centres.	Moving data centres to increase resilience. Planning in place to move to an outsourced provider and infrastructure requirements will form part of this move.	Red
Swindon	Neutral	Loss of stock supply to branches	Alternate warehouse provision and systems	Swansea identified as potential recovery area but not tested, systems to be made resilient and recovery proven.	Red

POL00423567

Systems	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Verizon	Averse	Loss of all branch operations. Loss of all other business operations.	Zero down time	TBC. Many failures with Verizon across 2018 which have stablised recently. IT to confirm the resilience in the Verizon network for continual service and to confirm the disaster recovrey time should key component areas of Verizon be lost.	TBC
Call Centre ACD/IVR	Averse	Loss of ability to manage calls to NBSC	2 hour recovery time	TBC. Will be picked up in the Verizon / Puzzel resilience review.	TBC
Call Centre systems (Dynamics)	Averse	Loss of ability to respond in a coordinated manner to incoming NBSC calls	2 hour recovery time	TBC. Working with NBSC and IT to confirm.	TBC
Horizon	Averse	Loss of all branch operations.	Zero down time	The Horizon database for branches has been recovered in a successful test in 2018. A full datacentre test can not be run due to the age of POLSAP equipment in the same datacentre. There is a contracted 2 hour recovery time for POCA / Banking / Vocalink and debit card payments which can be met. All other Horizon services are contracted for a 5 hour recovery. Moving to the cloud which will increase operational resilience and build confidence but still with a 5 hour contracted recovery time for disaster recovery.	Red / Amber
Polsap	Neutral	Loss of key central system	Recovery within 2 working days	Not tested for five years, moving to new systems and location in late January 2019	Green in Feb 2019
CFS	Neutral	Loss of key central system	Recovery within 2 working days	To be confirmed	TBC
APOP	Neutral	Loss of payments out system	Recovery within 2 working days	To be confirmed	TBC
Swindon Stock systems	Neutral	Loss of warehouse stock control	Recovery within 2 working days	To be confirmed	TBC

POL00423567

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
POI Call Centre	Averse	Unable to manage incoming customer calls	Alternative recovery site	TBC. Working with POI on the plans for Glasgow.	TBC
Payzone	Averse	Unable to support outlets using Payzone technology	Alternative recovery office.	Currently reliant on the good will of the old holding company and for them to free up space. This is untested. Planning to move to a Sungard solution by June 2019.	Red

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
IT Suppliers (to be broken down as the work continues. Will include Fujitsu, Computacenter, ATOS, Accenture etc)	Averse	Unable to deliver system support to Post Office systems	Zero down time	TBC. This appetite is the impact on the business not on IT operations and as such there is work to ensure the IT assumptions align with the business needs. The supplier risk here is on the business support provided to IT by suppliers, not the technical delivery of systems. IT have confirmed there is a varying level of disaster recovery testing in place across all suppliers and a regulary monthy review of progress. BC team is working with IT on the detailed level of this and how it meets business needs. This item will be broken down into each supplier as the information is confirmed.	TBC
DWP	Averse	Unable to deliver POCA support	2 hour recovery time	TBC Working with the POCA team	TBC
Ingenico	Averse	Unable to process card payments	2 hour recovery time	TBC Contract states there is recovery capability in place but further evidence that this meets business needs is required.	TBC
Grapevine	Averse	Unable to provide security support for branches. Unable to support all crisis response tools in place for Post Office. Unable to support evacuation process. Unable to communicate to all branches.	Zero down time, resilient systems, alternative office space.	Page One (underlying system) failed in late 2018 and was down for over 2 hours which presented a problem to Post Office. Other resilience is in place but further testing of the systems is required. Working with Grapevine to liaise with Page One over resilience levels.	Red
CBRE	Averse	Unable to respond to building issues	Intra day recovery times	TBC working with facilities team	TBC
Servest	Averse	Unable to support the management of key locations	Intra day recovery times	TBC working with facilities team	TBC

POL00423567

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Banks	Neutral	Unable to deliver support to operations externally to support the Banking Framework	Intra day recovery times	All Banks are contracted to provide this but evidence of testing of this capability has not been seen. Post Office relies on the Banks to process incoming cheques and confirm incoming and outgoing monies. They also process the incoming cheques. If they were not available for 2 days branches would continue to serve customers but Post Office finance operations and confidence would weaken over time.	TBC

POL00423567

Business Continuity Risk Appetite Off-Risk Programme – Green / Amber

The tables below show the key areas of Post Office where the current contingency solutions or resilience levels are shown in the Strategy Status as meeting business needs or are in place but need some further work.

Risk Appetite Table

Locations	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Supply Chain Depots	Averse	Loss of depot or cash centre, loss of supply or collection of cash to branches.	Alternate depots and cash centre processing equipment	Resilient depots and identified third party depots.	Amber
Chesterfield	Averse	Loss of Branch support Call Centre, Treasury and Finance Service Centre	Recovery Office	Sungard solution in place and tested	Green
Bristol	Averse	Loss of cash ordering process	Recovery Office	Sungard solution in place and tested	Green
Computacenter DC	Averse	Loss of key systems	Resilient design with zero down time and disaster recovery solutions	Full datacentre test run in 2018 successfully. Regular and ongoing component tests undertaken.	Green
Accenture DC	Averse	Loss of key systems	Resilient design with zero down time and disaster recovery solutions	Datacentre test run in 2017 successfully. Regular and ongoing component tests undertaken.	Green
Verizon DC	Averse	Loss of network and Puzzel ACD IVR Call Centre systems	Resilient design with zero down time and disaster recovery solutions	Datacentre test run in 2017 successfully. Regular and ongoing component tests undertaken.	Green
Finsbury Dials	Tolerant	Loss of head office functions and strategic leadership	Home working capability and recovery office	Home working solution proven and Sungard solution in place.	Green / Amber
Bolton	Tolerant	Loss of internal human resources support services	Recovery Office	Sungard solution in place and tested	Green

POL00423567

Systems	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Other Central Systems (To be broken down as the work continues, includes Credence, POLSAP, SuccessFactors, CFS etc)	Tolerant	Loss of support systems to operations, back office systems and financial systems.	Intra day recovery times	Systems have 4 hour contracted recovery times. POLSAP has not been tested for 5 years but should be moved to a new application by Feb 2019. Other systems run annual disaster recovery tests and meet the 4 hour target. Manual operations are in place to cover the down time and are proven. Further work with IT required to determine the levels of DR testing undertaken to prove the assumptions.	Green post Jan 2019
Email	Neutral	Loss of key communication tool.	Intra day recovery time	Technology is in place to provide robust email. Use of webmail in extremis is possible. Testing of this has not been undertaken. Mimecast can deliver a solution to this and testing of this should be undertaken.	Amber
Office Systems	Tolerant	Loss of day to day work tools	Intra day recovery times	Computacenter have run a full datacentre recovery test and restored systems to meet business needs.	Green
MDM	Neutral	Loss of key central system	Recovery within 2 working days	Succesful test in 2018 met business needs	Green
Credence	Neutral	Loss of key central system	Recovery within 2 working days	Succesful test in 2018 met business needs	Green

POL00423567

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Supply Chain	Averse	Unable to collect monies from branches Unable to deliver monies to branches Unable to replenish branch stock. Unable to fulfil Banking Framework	Alternate Depots, vehicles and cash processing capabilities within a working day.	Multiple depots across the UK can provide mutual support, as can alternative cash centres. Utilising third parties is also within current planning. Loss of Swindon is a single point of failure and plans for this are not tested.	Amber
NBSC	Averse	Unable to support branch operations	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Limited home working has also been tested.	Green
Communications	Averse	Unable to respond to any challenges	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
IT Management	Neutral	Unable to support contracts	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Finance Service Centre	Neutral	Unable to make payments or reconcile incoming monies	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Home working has also been tested. Manual work around for IT system failure in place.	Green
Treasury	Neutral	Unable to confirm funding requirements	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Home working has also been tested.	Green

POL00423567

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Mails Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Retail Management Team	Tolerant	Unable to support branch strategy	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Banking Framework Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Telco Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Bureau Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green

POL00423567

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Finance	Tolerant	Unable to provide financial updates	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
POI	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Bolton HRSC	Tolerant	Unable to respond to internal HR queries	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested.	Green
HR	Tolerant	Unable to support staffing needs	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
LRG	Tolerant	Unable to provide internal operational support	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green

POL00423567

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Royal Mail Group	Averse	Unable to collect from branches. Unable to deliver support to operations	Intra day recovery times	Greatest risk is strike for which Post Office and Royal Mail have worked together on identifying contingency solutions. Short term this would meet Post Office needs, within 3 days it would be difficult	Amber
VocaLink	Averse	Unable to provide ATM operations. Unable to provide faster payments.	2 hour recovery time	Three datacentres running continuously with load sharing. Zero down time tests run regularly. Observed testing and understanding has been shared with Post Office.	Green
FRES	Neutral	Unable to meet Bureau requirements	Recovery within 2 working days.	Some small stock holding within Supply Chain would mitigate a short down time. Recovery capability is tested but on the same campus.	Amber
Cardtronics	Neutral	Unable to meet ATM maintenance requirements	Recovery within 2 working days	ATM failures can be coped with for two days but after this repair and catch up of time lost would be essential.	Amber
Legal Advisors	Neutral	Unable to provide external legal advice	Recovery within 2 working days	Contractual recovery times and evidenced documentation meet Post Office needs.	Green

POL00423567

Post Office

Business Continuity Management Policy

8.2

1

POL00423567

Contents Page

POL00423567

Document Control Sheet

POLICY SUMMARY			
GE Policy Sponsor	**Policy Owner**	**Policy Implementor**	**Policy Approver(s)**
General Counsel **Jane MacLeod**	Business Continuity Manager **Tim Armit**	Business Continuity Manager **Tim Armit**	Post Office **RCC and ARC Committees**
Version and Status:	**Policy Review Period**	**Effective from :**	**Policy location:**
Final – v1.0	Annually from policy effective date	19th May 2016	Policy intranet page

DOCUMENT REVISION HISTORY			
Version	**Date**	**Author**	**Reason For Change**
V0.7	15/11/2016	**Georgina Blair**	Updated for name of new Business Continuity manager

POLICY APPROVAL		
Role/Forum	**Name**	**Date**
Executive Owner and Sponsor	**General Counsel (Jane MacLeod)**	30 March 2016
Executive Committee	**Post Office Risk and Compliance Committee (RCC)**	5 May 2016
Board Committee	**Post Office Audit, Risk and Compliance Committee (ARC)**	19 May 2016

DOCUMENT DISTRIBUTION STATUS			
Distribution (Mark x as appropriate)		Document Sensitivity (Mark x as appropriate)	
Internal Only	X	Non-sensitive	
External Only		Sensitive	X

QUALITY STATEMENT	
Quality Control	Next review date
This document is periodically reviewed and at least once each year starting from the last effective date. This policy has been reviewed against the latest Post Office policy standards.	No later than 19th May 2017

8.2

POL00423567

Section A. Introduction

Chief Executive's Note

Post Office Group ('Post Office') is committed to doing things correctly. Our Business Standards are our code of behaviours that represent the conduct we expect. This policy is directly related to this code ensuring the highest standards of business continuity management are maintained.

This policy sets out what is and is not acceptable but if you have any doubts or questions, these should be referred in the first instance to the policy owner, the Business Continuity Manager, who oversees compliance with this policy. It is essential that you read this policy.

Introduction by the Group Executive Policy Owner: General Counsel

As Post Office's General Counsel and the Group Executive Policy Owner I have overall accountability for business continuity management framework to the Board of Directors. Post Office's Audit, Risk and Compliance Committee considers business continuity as a standing agenda item and the Board is updated on a regular and timely basis.

POL00423567

Section B. Context

About this Policy

The purpose of this document is to define Post Office's policy with regard to business continuity management that is appropriate to the aims and objectives of Post Office. This includes:

- A framework for:
  - setting business continuity objectives;
  - satisfying appropriate requirements;
  - continual improvement of the Business Continuity Management Programme; and
- A high level statement of our key controls in respect of business continuity.

The Policy is consistent with business continuity "ISO22301", which are the Business Continuity Institute's Good Practice Guidelines.

Policy Scope: It is important to understand which areas of the business currently fall under the protection of the policy, and which do not. The boundaries of the Post Office business continuity framework are detailed within a separate document, "Business Continuity Context, Requirements and Scope", and these documents should be reviewed together when assessing a BC response requirement.

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

What is Business Continuity?

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

Risk Appetite

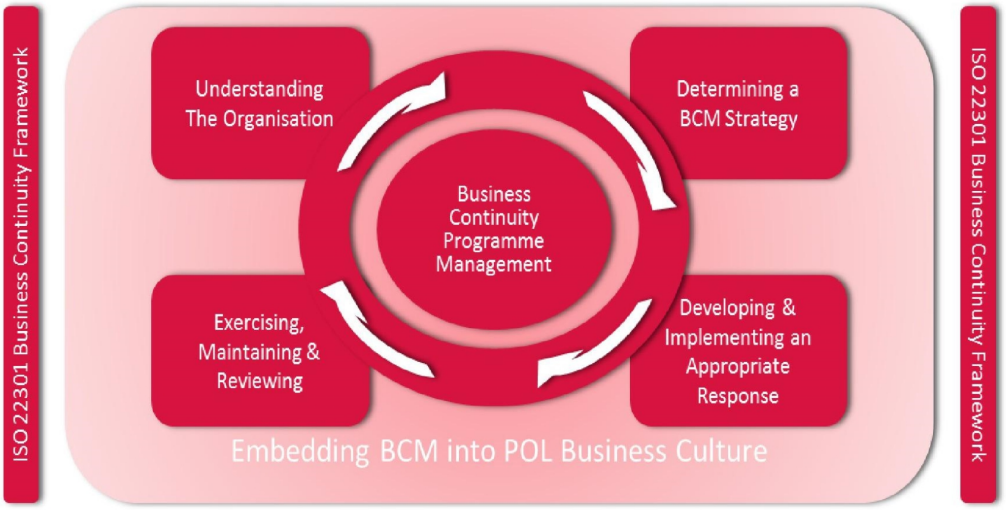
Post Office has an averse appetite for business continuity risk. Post Office recognises that it cannot completely eliminate this risk. However, this policy sets out controls to reduce and/ or mitigate such risks.

How we organise Business Continuity Management

This policy describes Post Office's Business Continuity Management policy and should be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

POL00423567

The BCM Framework



This Business Continuity Management Policy is stored electronically, and is available to all relevant stakeholders within the organisation.

8.2

6

POL00423567

Who is responsible

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

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for the day to day implementation of and compliance with this policy and is accountable in this regard to the General Counsel.

Who must comply and how

Compliance with this policy is mandatory for all Post Office employees, officers, contractors, casual workers and agency workers. This policy applies wherever in the world Post Office's business is undertaken. All third parties who do business with Post Office, including consultants, suppliers and business and franchise partners, will be asked to agree contractually to this policy or to comply with their own equivalent policy.

It is important that you read, understand and comply with this policy. Your actions, behaviour and conduct to apply the provisions of this policy are your responsibility.

You must adhere to all parts of this policy. You should avoid any activity which may lead to a breach of this policy. We may request your confirmation of agreement to this policy. You must notify your line manager, in the first instance, as soon as possible if you believe or suspect that a breach of this policy has occurred or may occur.

You may request a policy exception or waiver to this policy, but you must follow the Post Office's exceptions and waivers procedures which can be obtained from the business continuity Policy Owner.

If non-compliance is identified the matter must be referred to the General Counsel. Any investigations should be carried out in accordance with Investigations Policy. If the cause is found to be due to wilful disregard or negligence, it will be treated as a disciplinary offence.

POL00423567

Section C. Policy Details

Information

Post Office recognises the need to ensure that our business operates safely, smoothly and without interruption for the benefit of our colleagues, customers, shareholders and other stakeholders.

To ensure such levels of safe, continuous operation, Post Office has implemented a Business Continuity Framework consistent with "ISO 22301".

The operation of a Business Continuity Framework has many benefits for Post Office, including:

- The safe-guarding of colleagues at times of duress;
- Ensuring the supply of goods and services to our customer; Protection of revenue streams and business profitability;
- Maintenance and enhancement of shareholder / stakeholder value; and
- Compliance with legal and regulatory requirements.

In addition, our Business Continuity Framework is a commitment to the development, maintenance, improvement and socialisation of a Business Continuity Management Programme within and across the organisation.

Our controls and arrangements

1. Baseline and on-going Business Continuity objectives

The baseline objectives for business continuity within Post Office are defined within the "Business Continuity Context, Requirements and Scope" document. These are fundamental steps required which are led by business areas and are not subject to frequent change.

These baseline objectives guide the setting of lower level detail for short-term objectives for business continuity planning arrangements within an annual cycle. They coincide with the organisational budget planning. This ensures that adequate funding is obtained for necessary activities identified in the previous cycle.

These business continuity objectives will be documented in the Business Continuity Management Plan ("BCM Plan"), produced each financial year, which will also identify how objectives will be achieved, over what estimated period, and at what level of estimated cost. Once the annual BCM Plan is approved by the Post Office Risk and Compliance Committee it will be subject to regular management review to ensure that its objectives remain valid.

Amendments to objectives will be managed through the standard Post Office change management process.

POL00423567

2. Satisfying BCMP Requirements

Senior Managers commit to the provision of the appropriate resources to establish and develop the Business Continuity Management Programme ("BCMP").

Systematic performance review of the programme. This is conducted by the Business Continuity Manager on a regular basis, ensuring that quality objectives are being met. Qualitative evaluation is undertaken and any issues identified through the audit programme and management processes. Management review includes departmental and other management meetings.

Business Continuity Management Quality System. The Business Continuity Manager has overall authority and responsibility for this and implements and manages the system carrying out the following:

- The identification, documentation and fulfilment of applicable requirements;
- Assigning authorities and responsibilities for the implementation, management and improvement of the BCMP;
- Integration of business processes with the BCMP;
- Compliance with statutory, regulatory and contractual requirements in the management of assets used to deliver products and services; and
- Reporting to senior management on performance and improvement of the BCMP

Role definition and responsibilities are reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk.

Post Office will ensure that colleagues involved with the BCMP are competent on the basis of appropriate education, training, skills and experience. The skills are required to ensure business continuity will be determined and reviewed on a regular basis, together with an assessment of existing skill levels within Post Office. Training needs will be identified and executed via individual's training plans maintained to ensure that competences are in place.

Full details of the business continuity responsibilities associated with each of the required roles, and how they are associated within Post Office are given in a separate document, "Roles, Responsibilities and Authorities".

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. Where this involves the operation of a business process, or part of such process, that falls within the scope of the BCMP, then this should be identified by the Business Continuity Manager within the annual Business Continuity Management Plan.

Post Office retains governance of the relevant business continuity management processes for third parties by demonstrating:

- Accountability for the process;

POL00423567

- Control of the definition of, and interface to, the process;
- Performance and compliance monitoring; and
- Control over process improvements.

This will be evidenced by documentation and records, including contracts, meeting minutes and performance reports.

Third party agreement contractual business continuity terms. Specific, high level, requirements for new and existing relationships will be made available to associated third parties by the relevant third party relationship manager. These requirements set out minimum expectations for service continuity provision (as appropriate to the contractual service level terms). For further information see "Supplier Business Continuity Evaluation Process".

3. Approach to Managing Risk & Audit Requirements

The risk management strategy defined under ISO 22301 requires that relevant assets are identified and the following considerations made:

- Threats;
- Vulnerabilities;
- Impact & likelihood before risk treatment;
- Risk treatment (e.g. reduction, removal, transfer);
- Function responsible/ owner; and
- Timescale and review frequency.

Risk management will occur at multiple levels within the BCMP, including but not restricted to:

- Business continuity management planning – risks to the achievement of objectives;
- Business Continuity risk assessment;
- Assessment of the risk of changes under the established business change model; and
- At the project level as part of the management of significant business change.

High level risk assessments will be reviewed annually, or upon significant change to the business environment. More detail on the approach to risk assessment can be found in the document "Risk Assessment Process".

Regular reviews must take place concerning how well business continuity management processes and procedures are being observed. These occur at two levels:

- Structured regular management review of conformity to policies & procedures within Post Office; and
- Internal audit reviews against the ISO 22301 standard by the Post Office Internal Audit Team.

POL00423567

Certification auditing. Additionally, should certification to ISO 22301 be sought and attained, a third audit level applies:

- External audit against the standard in order to gain and maintain certification to ISO 22301.

Details on the process for internal audits can be found in the document "Procedure for Business Continuity Audits".

4. Continual Service Improvement

The approach to continual improvement of the BCMP is to:

- Consider effectiveness across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- increase the level of proactivity (and the business perception of proactivity) with regard to the on-going management of business continuity;
- Achieve an enhanced understanding of and relationship with the business units to which the BCMP applies;
- Review relevant metrics on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback;
- Obtain ideas for improvement via regular review meetings with stakeholders, documenting them in the "Procedure for Continual Improvement"; and
- Review the "Procedure for Continual Improvement" document at regular management meetings in order to prioritise and assess timescales and benefits.

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

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

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

Accepted improvement proposals will be prioritised, and planned according to standard project management principals. Additional information on continual improvement methodology can be found in "Procedure for Continual Improvement".

POL00423567

Section D. Governance

How we monitor compliance

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

Review and assessment of compliance with this policy is done on a timely basis and regular gap analysis is undertaken by the Business Continuity Manager and reported to the Risk and Compliance Committee.

Business continuity testing is planned and pre-determined. See further information in the "Business Continuity Exercising and Testing Schedule". Post Office's capability to maintain business operation will be subjected to exercise, and the results of these exercises will also be made available to the Risk and Compliance Committee.

We require third parties who do business with Post Office to have at least equivalent arrangements, systems and controls to this policy, and these should be demonstrable on request.

How to raise a concern

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

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or,
- bring it to Post Office's attention independently of management, via the Speak Up Line (see Section E 'References' for more information).

Contact us and more information

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

POL00423567

Section E. Key Terms and References

Key Terms

Term or Acronym	Description
Post Office Group ('Post Office')	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services (POMS)
Executive Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document V0.5
ISO 22301	The International Standard for Societal Security (Business Continuity).

References

References	Description
Business Continuity Context, Requirements and Scope	The purpose of this document is to describe the way the business operates, internal and external factors influencing it and to highlight in general terms the potential consequences of a business interruption. This will allow the most appropriate level of measures to be put in place to reduce the level of risk and to ensure that plans are available and tested to manage the impact of any interruptions that do occur.
Roles, Responsibilities and Authorities	The purpose of this document is to set out the organisation structure in terms of job roles, management and numbers of resources in each area and then to define how responsibility for each of the processes within the Business Continuity Management System (BCMS) is allocated within that structure.
Supplier Business Continuity Evaluation Process	This document sets out a process for the evaluation of the business continuity arrangements of our suppliers so that a degree of confidence may be gained that

POL00423567

	they possess sufficient resilience to support our requirements.
Risk Assessment Process	It is important that Post Office has an effective risk assessment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them. The starting point for risk assessment is the list of key business activities documented in the most recent business impact analysis.
Procedure for Business Continuity Audits	The purpose of this document is to set out how the Business Continuity Management Quality system will be audited internally.
Continual Improvement Action Log	Management of BCMP improvements can become unwieldy if they are spread across multiple reports, action plans and meeting minutes. The idea of this spreadsheet is to act as a focal point to record, assess and track all such improvement items in a common manner.
Procedure for Continual Improvement	In general Post Office will use the Plan-Do-Check-Act method (the Deming Cycle) for managing improvements as defined in the ISO 22301 standard
Business Continuity Exercising and Testing Schedule	The purpose of this document is to set out a schedule for testing / exercising activities.
Whistleblowing (Speak Up Line)	In case of concerns staff may contact their line manager, a senior member of the HR Team, or if either or both are not available staff can contact Post Office's General Counsel, Jane MacLeod who can be contacted by email on: whistleblowing GRO or by telephone on: GRO Alternatively staff can use the Speak Up service available on GRO or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

POL00423567

UK Data Protection Act (incorporating GDPR) Compliance Status Report

Authors: Clare Hammond Sponsor: Jane Macleod Meeting date: 9th May 2019

Document Version: Final

Executive Summary

Context

- The UK Data Protection Act 2018 (UK DPA 18) came into force in May 2018 replacing the UK Data Protection Act 1998 (UK DPA 98) and incorporates the EU General Data Protection Regulation (GDPR) along with UK specific exemptions and interpretations. The legislation builds on the foundation of UK DPA 98 and includes increased penalties for non-compliance (up to 4% of global annual turnover) and a requirement that organisations demonstrate accountability. The Information Commissioner's Office (ICO) is the UK Data Protection Authority, which enforces the UK DPA 18 and regulates Post Office.
- It is important to recognise that Post Office processes personal data in a uniquely complex environment. Information is processed on behalf of more than 140 different data controllers, including banks and government agencies. Post Office uses more than 170 different data processors, who process personal data on behalf of Post Office.
- Given the importance of trust to the Post Office brand, it is imperative that Post Office does, and is seen to, protect all personal data relating to customers, agents, employees and any other data subjects whose data is processed.
- The Post Office GDPR Programme ran from early 2017 and closed in April 2019 and was intended to achieve 'effective compliance[1]' by May 2018 and 'substantive compliance[2]' by the close of the programme. It is important that ongoing compliance is monitored, improved and sustained as we move into 'business as usual'.
- This paper is an assessment by the Data Protection Team of the level of compliance achieved by the GDPR Programme in the context of Post Office's risk appetite.

9

Questions this paper addresses

- What level of compliance with the UK DPA 18 has Post Office achieved and is this within Post Office's risk appetite?
- What further actions are needed to ensure that Post Office achieves and sustains the required level of compliance?
- What structures are in place to monitor, improve and report compliance to the UK DPA 18 in a 'business as usual' setting?

[1] *As defined by the GDPR Business case 04/18 covering aspects visible to data subjects.*
[2] *As defined by the GDPR Business case 04/18 covering other aspects.*

POL00423567

Conclusion

1. The GDPR Programme, working with the Data Protection Team, has delivered a robust compliance position that provides a foundation to enable Post Office to continue to improve. A maturity model has been used to assess the level of compliance and shows that the current status is an 'Active' light green progressing to the desired state 'Proactive' dark green. The status in May 2017, before the GDPR Programme was assessed as 'Reactive' amber.

2. There are two priority areas that require the Data Protection Team's focus over the next four months (to end September 2019); Data Protection Governance and Monitoring Data Handling Practices (i.e. audit and review). Other lower priority areas (e.g. third party risk and monitoring of new operational practices) are being reviewed with the aim of moving to a 'Proactive' rating by the end of 2019.

3. It is proposed that a quarterly 'Privacy Forum' is set up to enable Post Office to meet its Governance requirements and raise the profile of Data Protection within Post Office.

4. As Post Office is not yet at the target compliance maturity level, there is a risk of non-compliance which falls outside risk appetite. The gap is planned to be closed by the end of the year and the areas where work is required are not those that would attract the higher sanctions from the ICO. It is judged that our current level of compliance is above that of peer organisations.

5. Further actions required to bring Post Office's compliance to the UK DPA 18 to the target state have been identified, some of which are the responsibility of the wider organisation or are separate funded projects, for example, Records Retention.

Input Sought

RCC is requested to confirm support for the proposals included in this paper.

POL00423567

Report

What did the GDPR Programme highlight in terms of the Processing activities undertaken by Post Office?

1. Around 575 different processing activities have been identified and mapped as part of the GDPR Programme. Many of these have had data flow diagrams produced and all are inventoried within our One Trust Privacy Management system of record. The ICO has invited Post Office to discuss this complexity with them in order to benefit both organisations and any data subjects who contact them directly. They are particularly interested in how responsibilities are split with Royal Mail and the DPOs of both companies are in discussions with the ICO about facilitating this discussion.

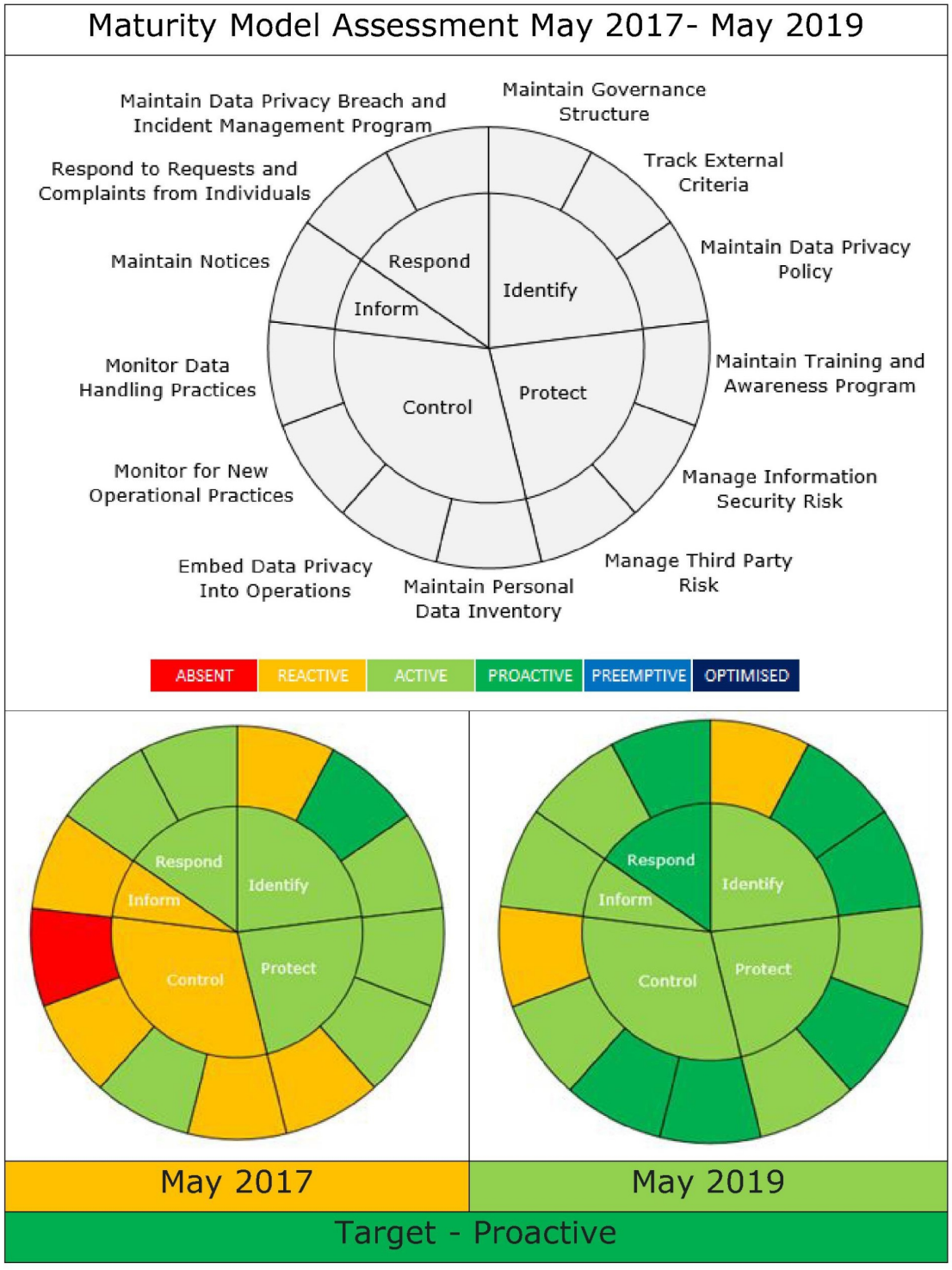
What is the basis of this Analysis of Compliance?

2. The Post Office Data Protection Framework has been defined and is based upon the Nymity[3] Accountability model which is recognised as industry good practice. All relevant Articles of the GDPR are mapped to Privacy Management categories and activities, which in turn have been mapped to the new draft NIST (National Institute of Standards and Technology) Privacy 'functions'. It is proposed that progress will be monitored on a regular basis within a new Privacy Forum. A Privacy Dashboard is being developed, by the end of June, to track key management information and output measures such as incidents, complaints, requests and training completions etc.

3. The following diagram shows the 13 categories of the Privacy Framework around the outer wheel, mapped to the 5 NIST 'functions'. The segments are colour coded according to the maturity as per the key. Full definitions of each level are in the Appendix. The levels have been judged by the Data Protection team with input from relevant areas (e.g. IT Security).

[3] The Nymity Privacy Management Accountability Framework™ is the de facto industry standard framework for privacy management, and contains over 130 privacy management activities organised into 13 categories.

POL00423567



9

POL00423567

How was 'Proactive' determined to be the desired level of the Maturity Model and how does this fit with Risk Appetite?

4. 'Proactive' is defined as having a well-documented approach, consistently applied; having activities occur on a regular, planned basis with failures identified and rectified. A balance has been applied that provides for a robust, defendable position that protects Post Office's personal data while not overburdening the organisation.

5. Post Office's 'Protecting Personal Data Policy' describes the Post Office as having a:

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

   Adverse risk appetite for
   - litigation in relation to high profile cases/issues
   - not complying with law and regulations or deviation from business conduct standards
   - data loss/leakage that can lead to customer, commercial or reputational damage
   - inaccurate and unreliable processing of data

   A maturity level of 'Proactive' has been judged to sit within risk appetite.

How does the model work?

6. Each category contains a number of activities that range from 'essential for compliance' and mapped to a GDPR Article to 'enhancing' and good practice. Each activity has equal weighting within a category.

7. It is proposed that the Data Protection Team will re-evaluate the maturity score every quarter, and present at the Privacy Forum and maintain a database of evidence of controls.

Proposed actions needed to move the status of 'Maintain Governance Structure' to 'Proactive'?

8. Governance structures, including the establishment of a regular Privacy Forum with terms of reference, need to be defined and implemented. Key management information within a dashboard are planned to be available to internal stakeholders on a monthly basis and reported to the Forum quarterly.

9. The Data Protection Team will work with the Policy Governance manager to develop good accountability and governance structures so that ownership of policies, processes, contracts and assets is well defined and responsibilities understood throughout the organisation.

10. It is proposed that we establish a network of 'data privacy champions' throughout the organisation. The face to face GDPR training that was undertaken in 2018 demonstrated that there are a number of individuals who have a keen interest in the topic and would like to be a key contact for their area of the business.

POL00423567

Proposed actions needed to move the status of 'Monitor Data Handling Practices' to 'Proactive'?

11. A review of Data Protection has been included in the 2019/20 Internal Audit plan. The objective of this review is to assess the operational effectiveness of the structure, process and controls in place to ensure ongoing GDPR compliance. In addition Internal Audit will follow up the actions from the 2017/18 GDPR programme review to ensure those controls are embedded and sustainable.

12. The Data Protection Team will be establishing a programme of informal 'Privacy Reviews' and walk-throughs targeting key areas of the business. This will be risk based and could be as a result of an incident (or series of regular low level incidents) or target groups who process particularly sensitive personal data.

Proposed actions needed to move the status of the other categories to 'Proactive'?

13. While there is a robust annual training course that all staff are required to take, further awareness materials will be developed and regular communication undertaken through the Comms team. It is desirable to have other regular events and the Data Protection Team will be assessing whether an annual 'Privacy Day' can be established.

14. The Third Party Risk Assessment process is established and focusses on the IT Security of key vendors. The Risk team has agreed to include Data Protection as part of the reviews and assessments. In addition, an ongoing due diligence process should be established that requires higher risk processors to regularly report their compliance status and to demonstrate adherence to key contractual terms.

15. Data Protection by Design processes will be evaluated to identify enhancements that can be made to ensure that Data Protection is considered and built into every stage of a product or process development. The Data Protection team has made significant progress by building more effective working relationships with the business teams. However this requires formalising and documenting, particularly as the organisation embraces Agile ways of working.

16. Privacy Notices are in place for all key groups of data subjects. There remain some gaps, in particular, how to deliver information to customers in a Branch setting. In addition, a regular review and sign off process will be established to ensure that all Privacy Notices are in line with the recent ICO guidance.

17. Complaint and enquiry handling from data subjects, particularly customers, is handled and tracked, however enhancements are needed in order to ensure that the processes are repeatable and measurable. It is clear through recent ICO enquiries, that not all complaints that come in from customers make it to the Data Protection team (e.g. marketing complaints and challenges over use of personal data) and additional processes and training need to be put in place to ensure that all possible 'entry/capture' points (of which there are many) are aware of Post Office's responsibilities.

POL00423567

What other key funded projects are required to deliver compliance to UK DPA 18?

18. The following projects are underway, which will support Post Office's compliance with UK DPA 18:

19. Records retention; it is critical to UK DPA 18 compliance that the project continues to establish retention schedules and system and process owners implement the required deletion procedures.

20. Continuing remediation of key contracts; the Legal Team, supported by external counsel, continue to work through the remediation of material contracts. Considerable progress has been made to date with all new contracts since May 2018 using the new GDPR templates.

21. The Joiners, Movers, Leavers (JML) project; this is a key project that is ensuring that only people who need access to personal data in order to do their job, have access. Some higher risk systems are moving to single sign on and others to enhanced manual access controls. The project will also recommend some lower risk systems that should implement stronger access controls. The project will close mid-July.

Next Steps

22. An agreement in principle is requested from this RCC group that allows the establishment of a quarterly Privacy Forum. It is envisaged that the first meeting of this group will be in September. Terms of Reference will be drafted and agreed at the first meeting.

23. A Privacy Dashboard and other metrics will be developed by the end of June and circulated to key internal stakeholders.

24. A comprehensive action plan will be developed by the end of June that includes all the proposals in this paper. This will move Post Office to a maturity level of 'Proactive' by the end of 2019.

Conclusion

25. The key takeaway is that Post Office's compliance to the UK DPA 18 is green moving to dark green. Given the adverse risk appetite for Data Protection compliance within Post Office, the current status is slightly below where we need to be.

26. With the agreement of RCC to the proposals within this paper, Post Office will move to a 'Proactive' dark green maturity position and be firmly within risk appetite.

POL00423567

Appendix

Definition of Maturity Levels

Maturity Levels		
Score	Level	Definition
0	ABSENT	Absence or only partially present.
1	REACTIVE	Inconsistent approach; Ad-hoc, undocumented procedures; Few records kept.
2	ACTIVE	Formally resourced; Objectives are defined; Procedures defined, but are applied inconsistently.
3	PROACTIVE	Well documented approach, consistently applied; Activities occur on a regular, planned basis; Failures are identified and rectified.
4	PREEMPTIVE	Consistent and robust application; Activities are increasingly automated; Processes and tools are integrated.
5	OPTIMISED	Processes are well managed and governed by leadership; Improvements are actively sought; Monitoring captures metric to measure performance.

POL00423567

Audit, Risk and Compliance Committee Agenda

Date:	Wednesday 29 May 2019	Time	14.00 – 16.30 hrs	Location	1.19 Wakefield

Present	Other Attendees	
• Carla Stent (Chair) • Tom Cooper • Tim Franklin • Ken McCall	• Alisdair Cameron (Interim CEO) • Shirine Khoury-Haq (Non-Executive Director) • Tim Parker (Chairman – PO Limited) • Andrew Paynter, PwC – by telephone (External Audit Partner) • [Additional PWC attendees TBC] • Amanda Bowe (item 2.) (Chair, ARC PO Insurance)	• Johann Appel (Head of Internal Audit) • Deana Hurley (Senior Manager, Assurance, deputising for Jenny Ellwood) • Jonathan Hill (Compliance Director) • Veronica Branton (Head of Secretariat) • Rob Houghton (item 9.) (Group COO) • David Parry (Senior Assistant Company Secretary)
Apology: Jenny Ellwood	• Liz Robson (items 5, 9.) (Change and IT Director – Retail) • Micheal Passmore (item 4.) (Change and IT Director – Retail)	• Mick Mitchell (item 9.) (IT Security & Service Director) • Ben Cooke (item 10.) (CIO - Back Office)

	Agenda Item	Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest** [Email from Carla to Veronica 25/03/19 of standing items and order]	Noting	Chair	
2.	**Update from Subsidiaries:** • Post Office Management Services ARC (Verbal) [Email from Carla to Veronica 25/03/19 of standing items and order]	Noting & Input	Amanda Bowe	14.00 – 14.05
3.	**Minutes and Matters Arising** [Email from Carla to Veronica 25/03/19 of standing items and order]	Approval	Chair	14.05 – 14.10
3.1	Minutes of the Audit, Risk and Compliance meeting held on 25 March 2019			
3.2	Actions List	Noting & Input		
3.3	Draft Minutes of the Risk and Compliance Committee held on 9 May 2019	Noting		
4.	**Annual Report and Accounts External Audit**	Approval	Micheal Passmore / Andrew Paynter (PwC)	14.10 – 15.00
4.1	ARA Covering Note			
4.2	Financial Statements			
4.3	Post Office Limited Briefing Book including Accounting Judgements			
4.4	PwC External Audit			
5.	**PCI-DSS Update**	Noting	Liz Robson	15.10 – 14.20
6.	**Internal Audit** [Email from Carla to Veronica 25/03/19 of standing items and order]	Noting & Input	Johann Appel	15.10 – 15.30
6.1	Internal Audit Report			

10

POL00423567

Audit, Risk and Compliance Committee Agenda

7.	**Risk** [Email from Carla to Veronica 25/03/19 of standing items and order]	Noting & Input	Deana Hurley	15.30– 15.50
7.1	Risk Report *Includes deep dive on Financial crime.* [request from ARC 25/03/19 to consider severity of risk, taken from notes of meeting with Jono, Johann & Jenny]			
7.2	Risk Management Section for Annual Report and Accounts [Jenny Ellwood email]			
8.	**Compliance** [Email from Carla to Veronica 25/03/19 of standing items and order]	Noting & Input	Jonathan Hill	15.50 – 16.10
8.1	Compliance Report *Including an update on Fit & Proper*			
9.	**Information Security Update** [Email from Carla to Veronica 25/03/19 of standing items and order] *Cyber Security Report* *Information Security Committee update [request from ARC 25/03/19]* *Security Strategy*	Noting & Input	Rob Houghton/ Mick Mitchell/Liz Robson	16.10 – 16.20
10.	**Back Office Transformation update** [update request ARC, actions 25/03/19]	Noting	Ben Cooke	16.20 – 16.25
11.	**Any other Business** Note: Date of next meeting 29 July 2019, 15.30 – 17.30 hrs	Noting	Chair	16.25 – 16.30

10