POL00423571

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	12 November 2020
Time:	11.00 - 14.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chairman)	Johann Appel (Head of Internal Audit)
Lisa Cherry (Group Chief People Officer)	Mark Baldock (Head of Risk)
Ben Foat (Group General Counsel)	Jonathan Hill (Compliance Director)
Amanda Jones (Group Retail and Franchise Network Director, Interim)	Tom Lee (Head of Finance Financial Accounting and Controls)
Cathy Mayor (Finance Director, Commercial) (deputising for Owen Woodley)	Rebecca Whibley (Senior Assistant Company Secretary)
Jeff Smyth (Group Chief Information Officer, Interim)	Helen Rhodes (People Shared Services Director) (observing)
Tim Perkins (Head of Security, Safety & Loss Prevention)[1]	Meredith Sharples (Director of Telecoms): Item 3.2
	Tony Jowett (Chief Information Security Officer): Item 4
	Rob Wilkins (Cloud Services Director): Item 4
	Mark Underwood (LCG Operations Director): Item 5
	Christine Kirby (Financial Controls Manager): item 7
	Brian Kelly (Finance Director - Tax, Treasury and Working Capital): Item 8
	Declan Salter (GLO Director): Item 9
	Graham Hemingway (Historical Matters Portfolio Lead): Item 9
	Ed Dutton (Post Office Insurance Managing Director): Item 10
	Karl Oliver (Head of Commercial Partnerships): Item 12
	Dan Zinner (Group Chief Strategy and Transformation Officer): Item 13
	Saira Burwood (Head of SPO): Item 13
	Andrew Goddard (Payzone MD): Item 14
	Sarah Gray (Group Legal Director): Item 15
	Rod Williams (Head of Legal, DR & Brand): Item 16
	Barbara Brannon (Procurement Director): Item 17
	Ed Dyer (Working Capital and Cash Management Lead): Item 19
Apologies:	
Owen Woodley (Group Chief Commercial Officer)	Nick Read (Group CEO)
Dial In Details:	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: 478 651 766# Pin (if applicable): 58042	

Time		Item		Owner	Action
11:00	1.	Welcome & Conflicts of Interest		Chair	Noting
	2.	Previous Meetings		Chair	
		2.1	Minutes (10 September 2020)		Approval
		2.2	Action List		Discussion
11:05	3.	Combined Risk, Compliance and Audit Update			

[1] Tim Perkins has taken over from Julie Thomas and will sit on the Committee in her place moving forwards.

Strictly Confidential

POL00423571

POST OFFICE LIMITED

		3.1	Risk Report (dashboard)	Mark Baldock	Noting (for onward submission to ARC)
		3.1.1	Risk Policy, including the proposed approach to Risk Appetite & Key Risk Indicators		Noting & Approval (for onward submission to ARC)
11:15		3.2	Compliance Report	Jonathan Hill	Noting (onward submission to ARC)
11:25		3.3	Internal Audit Report	Johann Appel	Noting (onward submission to ARC)
11:35	4.	PCI-DSS and Cyber Security Update			Noting (onward submission to ARC for information only)
		4.1	PCI-DSS	Jeff Smyth & Rob Wilkins	
		4.2	Cyber Security	Tony Jowett	
		4.3	Joiners, movers, leavers	Tony Jowett	
		4.4	Belfast Datacenter (Horizon) Disaster Recovery Post Test Briefing	Gary Walker	
11:45	5.	Suspense Accounts *There is an additional paper for this item in the Reading Room.*		Mark Underwood	Noting (onward submission to ARC)
11:55	6.	Notification of Transaction Correction error		Tim Perkins	Noting
12:05	7.	Financial Reporting Controls Framework Update		Tom Lee & Christine Kirby	Noting (onward submission to ARC)
12:15	8.	Agreed Upon Procedures		Tom Lee & Brian Kelly	Noting (onward submission to ARC, for information only)
12:25	9.	Historical Matters Unit (HMU) Governance Review		Graham Hemingway & Declan Salter	Noting (onward submission to ARC)
12:35	10.	Post Office Insurance Financial Conduct Authority Dual Pricing Change Impact		Ed Dutton	Noting (onward submission to ARC)
12:45	11.	Committee Terms of Reference		Chair/Secretary	Approval (onward submission to GE)
12:50	12.	Deepdive: Multiple Partner financial stability update		Amanda Jones & Karl Oliver	Noting (onward submission to ARC)
13:05	13.	Deepdive: Transformation Office Change Update 2020 *There are additional papers for this item in the Reading Room.*		Dan Zinner/Saira Burwood	Noting (onward submission to ARC)
13:20	14.	Payzone Risk Report		Andrew Goddard	Noting (onward submission to ARC)

Strictly Confidential

POL00423571

POST OFFICE LIMITED

13:30	15.	Law & Trends Update	Sarah Gray & Ben Foat	Noting (onward submission to ARC)
13:35	16.	Data Governance	Jonathan Hill & Rod Williams	Noting (onward submission to ARC, for information only)
13:45	17.	Procurement Governance & Compliance Report, including Barclays Bulk Cheque Processing Contract Extension (outstanding GE Paper)	Barbara Brannon	Noting & Approval (onward submission to ARC)
13:50	18.	Policies for Approval: *The policies may be found in the Reading Room.*	Jonathan Hill	Approval (onward submission to ARC via written resolution)
		18.1 Summary Paper		
		18.2 Change Management		
		18.3 Conflicts of Interest		
		18.4 Protecting Personal Data		
		18.5 Freedom of Information & Environmental Information Regulations		
13:55	19.	Directors & Officers Insurance Renewal	Ed Dyer	Noting (onward submission to ARC via action update and reading room)
14:00	21.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 24 November 2020	Chair	Noting
	20.	Any other business	Chair	Noting
Next RCC Meeting: Tuesday 12 January 2021 at 14.00 to 17.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ				

POL00423571

2.1

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance Committee ("RCC") meeting held via Microsoft Teams
on 10 September 2020 at 14:00

Present:	Alisdair Cameron (Chair) (AC)	Group Chief Financial Officer	
	Ben Foat (BF)	Group General Counsel	
	Amanda Jones (AJ)	Group Retail and Franchise Network Director, Interim	
	Lisa Cherry (LC)	Group Chief People Officer	
	Jeff Smyth (JS)	Group Chief Information Officer, Interim	
	Julie Thomas (JT)	Operations Director	
	Chrysanthy Pispinis (CP)	Post Office Money Director, Post Office	
In Attendance:	Johann Appel (JA)	Head of Internal Audit	
	Mark Baldock (MB)	Head of Risk	
	Jonathan Hill (JH)	Compliance Director	
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls	
	David Parry (DP)	Senior Assistant Company Secretary	
	Rebecca Whibley	Assistant Company Secretary	
	Maxine Cross (MC)	Head of Reward & Pensions, Reward & Pensions	Item 4
	Daisie Jope	Head of Organisational Effectiveness	Item 5
	Scott Robbins	Organisational Effectiveness Lead	Item 5
	Tony Jowett (TJ)	Chief Information Security Officer	Item 6
	Joseph Moussalli (JM)	Programme Manager, Project Managers and PMOs	Item 6
	Rob Wilkins (RW)	Cloud Services Director, MI, Data Strategy & Analytics	Item 6
	Mark Dixon	Treasurer	Item 7
	Andy Bear	Locktons (Account Manager)	Item 7
	Sarah I Gray (SIG)	Group Legal Director	Items 8, 9, 10
	Tim Perkins (TP)	Head of Security, Safety & Loss Prevention, Loss Prevention	Item 11
	Barbara Brannon	Procurement Director	Item 12
Apologies	Nick Read, Group CEO Owen Woodley, Group Chief Commercial Officer Cathy Mayor, Finance Director		

1.	**Welcome and Conflicts of Interest**	**Actions**
	The Chair opened the meeting and advised that all papers would be taken as read. No conflicts of interest were declared.	
2.	**Minutes and Action Lists**	
2.1	The minutes of the RCC meeting held 13 July 2020 were **APPROVED**.	
2.2	Progress on completion of actions as shown on the action log was **NOTED.**	
3.	**Risk, Compliance and Audit Update**	
	Risk	
3.1	MB presented the risk report. He explained the report was taken from the risks presented in Archer, and that his team would be meeting GE members/risk associates monthly to review departmental risks going forwards. An updated risk appetite statement (not updated since 2016) would be presented to the RCC, ARC and Board for formal sign-off in November, once reviewed against POL's new purpose (communicated to POL 8/9/20).	

POL00423571

3.2	He advised that the team had seen increased levels of engagement across the Group due to individual business units being more aware as the first line of defence, however risk articulation (being clear on the cause, event and impact of risk), alignment (ensuring risks are managed through Archer as a single source) and RAG ratings (to ensure they reflect Group standards) are areas for address.	
3.3	The Committee noted that there are 473 risks in the group (listed on Archer) with the following key enterprise risks: • Commercial – POL not an attractive business proposition due to complex/confusing products, new products considered cost ineffective and difficult to scale. • Covid-19 – the risk to business employees/postmasters and the business remain, particularly in light of reduced footfall/trading on the high street. • Financial – concern that funding is insufficient and costs uncontrolled in the short/medium/long term leading to the inability to deliver strategic objectives. • Legal – POL unable to comply with legislative and regulatory changes, resulting in fines, lost revenue, reputational and customer damage. It was noted that legal and regulatory updates would be provided to RCC to avoid this. The Committee requested further explanations be provided on the types of risks presented and advised that some risks had incorrect GE owners for example, AC was listed as risk owner for COVID. MB advised this would be reviewed with GE members.	
	Compliance	
3.4	JH presented the compliance report with the following points noted. **Telecoms**: JH reported that the regulator had agreed to stop fortnightly reporting following strong call centre performance during the COVID pandemic.	
3.5	**Fairness:** A meeting is planned shortly with NR, Meredith Sharples and Ofcom regarding POL's performance against the regulator's Farness Commitments (however JH questioned the need for NR to attend). The team is working on ways to reduce the number of 'vulnerable clients' and plans are to be presented to the regulator ahead of the meeting. Additionally, whilst not in breach with the regulator, the Telco team will be sending out Annual Best Tariff Notifications (required to be sent before 14 February 2021) to customers who have been out of contract for more than a year and have not received an End of Contract Notification. A rise in customer calls and complaints is expected as customers query why their current price is higher than the new offers presented in their communications.	
3.6	**GLO/Freedom of Information Requests/GDPR:** the team remains stretched responding to Historic Shortfall Scheme and related/linked FOI requests (186 open requests). Following receipt of 41 FOI enquiries considered vexatious from one journalist, 31,000 boxes of data (previously unknown) have now been identified in storage. These are being reviewed by legal, HSF and Peters and Peters and a separate paper for ARC will be prepared regarding this issue. The Committee recognised the need for improved data retention/management training across the group and in the retail network.	**Action: JH**
3.7	**Schrems II case and Privacy Shield:** the team is monitoring the implications for POL from Schrems II. There is the potential that POL will have to update its standard contractual clauses within its contracts where personal data is stored outside of the EEA. JH remarked this was an industry wide issue and which the team would continue to monitor.	
3.8	**Financial Crime:** there continues to be a large increase in suspicious activities reports during lockdown.	

POL00423571

	The team is working closely with the banks to understand the reasons for the continued spike. This remains a watching brief.	
	Internal Audit	
3.9	JA presented the IA report. Good progress has been made with the 2020/2021 IA programme with seven reviews (five in POL, two in POI) completed since the last ARC meeting in July, including a review of the Belfast exit programme. JA remarked there were no contentious issues to report and that the IA plan for 2020/21 would be reviewed against POL's new purpose.	
3.10	The Committee noted the following audits have been reviewed since the last ARC meeting (27/7/20): • GLO Historical Shortfall Scheme -Data Validation • Maintain Minimum Control Standards during Covid-19 (needs improvement) • RMPP (DB Pension Scheme) -Data Errors (Final Draft Report) (not rated, lessons learned) • Health & Safety Response to Covid-19 (Final Draft Report) (needs improvement) • Belfast Exit Programme Assurance –Phase 1 -Interim Report. JA reported there are three overdue actions which the team is following up. The Committee noted the need for management to respond to audit actions and take responsibility for completing their actions. The Risk, Compliance and Audit paper was **NOTED for onward submission to the ARC.**	
4.	**Pensions Assurance**	
4.1	LC and MC presented the Pensions Assurance paper.	
4.2	LC reported that since the last meeting, meetings have been held with the unions (who are keen to be actively involved in decisions related to claw back and reductions) and the Pensions Trustees. An Internal Audit has identified the following lessons learned: • The 2014 Robin Agreement was not effectively implemented. • The implementation of success factors in 2018 was to tight deadlines due to licences expiring. • There were insufficient controls in POL and RMPP to identify the errors that arose.	
4.3	Work to quantify the errors is expected to be completed by the mid-October September and communication with the Pension Trustees remains aligned. Annual Benefit Statements (ABS) for RMPPP members will be delayed and a holding statement to explain the delay sent to affected members (expected to be issued on or about 21 September 2020).	
4.4.	In view of the potential for leak, and the fact that pension statements have been delayed for a second successive year, LC advised that she had spoken to the Chair of ARC who had provided approval for a report to be made to the regulators ahead of ARC. The Committee requested a timetable and proposed quantum ahead of the ARC meeting, but noted that LC was due to meet the Chair of ARC separately to discuss this issue. The Pensions Assurance paper was **NOTED for onward submission to the ARC**.	**Action: LC/MC**
5.	**DeepDive: Successfactors**	
5.1	LC, DJ and SR presented the deepdive.	
5.2	LC reminded the Committee this was an outstanding request from the ARC - on whether the product was suitable for POL and that POL was making best use of the product. She had been in discussion with the Chair of ARC to discuss her findings and provide comfort to any risks.	

POL00423571

5.3	SR reported the product was considered a world leading system, but noted it was only as good as the design and implementation when initially installed/developed - implementation was challenging and the product has not been fully utilised.	
5.4	A review by Deloitte on Successfactors and the HR processes identified 51 new opportunities to improve the integrity of the system as well as functionality, connectivity, governance and reporting. Of the (See 51 opportunities, 21 'quick wins' were identified which can be delivered relatively easily with minimal cost. 22 opportunities were identified as 'Priority' based on value add and these have been 'combined' and worked up into 14 'prioritised opportunities'. Additionally, a HR Services Director has been brought on-board to focus on developing the HRSC and HR Service Delivery Model.	
5.5	The Committee noted the developments but recommended that consideration should be given to whether HR (particularly Payroll) could be outsourced; and that the report should clearly highlight the complexity of having differing types of pay within POL. The Deepdive Successfactors presentation was **NOTED for onward submission to the ARC**.	
6.	**PCI-DSS and Cyber Security Update**	
	PCI-DSS Programme Update	
6.1	RW presented the PCI-DSS update and reported the following: **P2PE workstream** (which encrypts retail and banking transactions from the Pin Entry Device (PED) to a PCI compliant zone in Ingenico before onward processing to Global Payments (retail transactions) or VocaLink (banking transactions): this remains on track to deliver per plan the Vocalink accreditation of the retail & banking software and is followed by a final round of testing and branch piloting activity to be completed by March 2021 (also on track). Once pilot activity is completed, the solution will be progressively rolled out across all branches with a full rollout and formal independent QSA accreditation being completed by June 2021. The team continues to investigate options to improve the velocity of the roll-out phase timelines. The TOM workstream (which addresses use of PCI data by POL in processes outside of the transactions occurring at the PED) has identified seven areas where changes to products and processes are required to achieve PCI compliance. The activity required to address each of these areas has been planned and the team is working with suppliers to achieve the required remediation.	
6.2	The following key updates since the last meeting were noted: • Fujitsu and Ingenico have completed the second banking key milestone: a balance enquiry, and the banking solution is on track to complete to plan. • Delivery of the payment solution has slipped by three weeks due to issues with the Global Payments test environment. Accreditation of the retail payment solution is now scheduled to complete in October (versus September). As this is not on the critical path there is no impact to the end to end plan. • Additional changes have been identified and the project team is working with the business to understand criticality and potential workarounds. Fujitsu and Ingenico are also impact assessing the changes in order that these can be delivered in future releases of the software. • Finances: We are currently tracking within the 2% tolerance on the £15.8m approved at board. However, some new risks have been identified that may need additional funds. • High Level Design now v2.4 has been updated with further TOM solutions.	

POL00423571

6.3	Although JS noted the slippage with the delivery of the payment solution, he remained confident all timelines and plans would be met on deadline. The Committee requested key milestones (including contractual milestones) be clearly highlighted in the paper for ARC. The PCI-DSS Programme Update was **NOTED for onward submission to the ARC.**	
	Cyber Security	
6.4	TJ presented the Cyber Security update. **Cyber Security Maturity**: Cyber security remains a key focus for the team. Since the last ARC meeting, business and IT strategies have been developing at pace and the team has adopted the following principles for the 2020/21 cyber programme: 1. Deliver maturity increases where there is greatest value for lowest cost –including Cyber Strategy and Policy developments plus other areas where we are making process-related changes. 2. Align as much as possible of the major cost items with delivery from other IT projects such as EUC, Belfast Exit where we will gain the capability as part of these projects. 3. Defer the remainder of the higher cost items for maturity increase. 4. Focus on security activities to enable the business such as those around SPM and Belfast Exit.	
6.5	Several capabilities (recommendations in the Deloitte Maturity assessments) have been deferred until beyond the end of FY2021. These include: 1. DLP (Data Loss Prevention) Phase 3 (Rule Enforcement) - DLP Phase 2 (analysis and pre enforcement activities) is still proceeding in 2020, and while full DLP maturity takes an average 2 years to achieve, deferring phase 3 until 2021 will add a further 6 months at a minimum to implementation timeline. 2. Network Access Control (NAC) – providing strong defences against unauthorised devices connecting to our network due to cost. 3. SOC Forensics – some of this capability will be provided by the GLO IT forensics team. 4. Firewall attestation capability enhancements enabling clear resolution of firewall rule issues. 5. Identity and Access Management automation. 6. SOC Room – unlikely to be needed for 6-12 months 7. Web Proxy enhancements – similar capability being developed under the EUC project. Additionally, the Central risk team is reviewing cyber risk appetite statements considering COVID working practices, the relaxation of certain controls for extensive remote work practices and the reduction in capex. Changes in risk appetite will result in changes to target maturity of cyber capabilities.	
6.6	**Covid-19:** ransomware attacks continue during Covid and Deloitte are reviewing the team's readiness for such an attack. The Committee noted that a major cyber security breach test would be completed in late 2020/early 2021, along with tower testing in October/November and a red team exercise.	
	Joiners Movers Leavers (JML)	
6.7	TJ presented the JML report. JML remains a key focus for the team, the biggest issue remains the different types of leaver (standard, extraordinary ie. those who receive a settlement, rapid i.e. disciplinary issue, and health related) and the associated tasks for each. Additionally contractual and leaving dates may differ taking into consideration leave taken during a notice period.	
6.8	TJ advised that an exercise for leavers completed during covid identified that IT access for all leavers was	

POL00423571

	removed on time, the HR leaving process was in all cases started on time and physical access and payroll were also terminated correctly for these leavers. However areas for improvement include the process for return of laptops and other kit, some leavers had deleted and downloaded confidential data, and the cleanliness of data in HR and IT systems.	
6.9	Two new responsibilities for JML will be introduced: an IT System Platform Owner (SPO) who will be responsible for the IT elements of a platform; and a Business Data Owner (BDO) from the owning business who will be accountable for the data in each system. Monthly reports on leavers will be provided to GE. The Committee noted the progress made and requested these be clearly articulated to ARC. The Cyber Security Update and JML report was **NOTED for onward submission to the ARC**.	
7.	**Insurance Renewal 2020/21**	
7.1	MD and AB (Locktons) presented the Insurance Renewal update. He reported that the renewal date is 1 November but given timings of the ARC meetings and the timetable for renewal (insurers will not give terms outside 30 days from renewal), final terms cannot be provided at this time. Delegated authority would be sought for the CEO and CFO to sign off the insurance renewal. As Locktons were procured compliantly (appointed initially for a 3 year term in 2015, extended for three further 12 month terms), legal and procurement agreed that an OJEU process for insurance renewal was not required. It was noted that Loctons are incentivised to keep POL's costs down.	
7.2	AB explained the 2019 renewal had seen difficult market conditions for crime and D&O lines and that premiums in 2019 had increased significantly to £1.6 million. Additionally POL had purchased further cyber coverage to mitigate against the increased volume of cyber-attacks. It was expected that premiums would increase again this year, due to challenging crime and D&O markets and concerns over COVID claims and whether appropriate coverage is in place. Consideration should be given as to whether to buy infectious disease coverage under Business Interruption. The Committee requested that all avenues be explored to reduce the premiums, particularly as working conditions this year had significantly changed. The Insurance Renewal Programme paper was **NOTED for onward submission to the ARC**.	
8.	**Law & Trends**	
8.1	SIG presented the Law Trends update. Although noting five matters (listed below) for the Committees' attention, the Committee discussed the impact of the Corporate Insolvency and Governance Act 2020 (the Act) to POL. SIG advised the Act had been fast tracked due to Covid and the potential of insolvency of suppliers. Most relevant to POL, is the wide-ranging prohibition on the operation of termination clauses in contracts for the supply of goods and/or services where the counterparty enters a relevant insolvency process. The new provisions would also prevent POL (as a supplier) from doing 'any other thing' (e.g. changing payment terms) where the client has entered into a relevant restructuring or insolvency process. However, POL could terminate a contract where a breach occurs after the insolvency procedure had	

POL00423571

	started. Certain exclusions apply e.g.to financial contracts. The Legal team are analysing excluded contracts . They are also conducting a review of key supplier contracts to identify those with narrowly drafted termination clauses where it might be prudent to monitor the financial health of the counterparty. Templates such as P- Suite documents, will be reviewed and updated accordingly.	
8.2	The following four matters were noted but not discussed in detail: 1. Court of Justice of the European Union (CJEU) - Schrems II Decision. 2. Ofcom Consultation – Implementing the new European Electronic Communications Code. 3. Online Platform Regulations. 4. HM Treasury consultation on new economic crime levy. The Law & Trends paper was **NOTED for onward submission to the ARC.**	
9.	**Bi-Annual Legal Risk Review (Non GLO/Starling)**	
9.1	SIG presented the Bi-Annual Legal Risk Review.	
9.2	She reported on the following key legal risks: • **Contract Management** – there are differing levels of expertise and management of contracts across the Group, specifically understanding the obligations of each party and the impact on POL. The Legal team has developed a contract management framework to improve standards required, and training will be provided to the business. Additional training to the legal team will be provided by external legal providers to improve knowledge/expertise, and an updated Procurement policy has been drafted for ARC for approval. The development of Web3 (contract management system) would ensure all contracts were centrally recorded and had named account owners. AC recommended the contract management process be automised as much as possible and suggested SIG discuss with TL the financial controls management system (Traction) to use as a template. • **Non-Compliance with Regulatory requirements and Principles** - there are varying levels of expertise across the Group regarding POL's regulatory obligations where activity is outsourced but not responsibility. Controls and accountabilities being mapped out by Compliance along with a review of policies is in place.	
9.3	BF noted that litigation was minimal save for GLO/Starling. The Bi-Annual Legal Risk Review was **NOTED for onward submission to the ARC**.	
10.	**Contract Management Framework (CMF)**	
10.1	SIG presented the Contract Management Framework update.	
10.2	She reported that against an initial target of 50 material contracts, that 132 of the 134 material contracts and 43 non material contracts have been located and uploaded onto Web3, with their obligations mapped and resource and processes have been agreed with Company Secretarial, Legal and Procurement to ensure new contracts, as entered into across the PO Group, are compliant with the CMF.	
10.3	The Legal team is working with Procurement to get the 1500 non-material contracts identified by GE and GE-1 uploaded to Web3 with header level details recorded. As contracts expire/ renew they will be fully	

POL00423571

	remediated (have their obligations mapped/ CM assigned) in line with ARC's direction in May. The project will stay open for the next nine months and will enable new contracts to be mapped, contract owners and managers identified, and compulsory training provided to the Group. The Committee recognised the importance of contract management. The Contract Management Framework (CMF) paper was **NOTED for onward submission to the ARC**	
11.	**Update on Post Master Accounts**	
11.1	TP presented the report. He explained this report arose from an ARC action to understand: 1) What information is presented to Post Masters regarding their customer accounts 2) What trends are prevalent or emerging in Postmaster customer accounts? 3) What further work can KPMG perform to assess whether any other product processes can give rise to similar issues to those identified with stamps? How much would this cost? What are the limitations and risks? Findings from reviewing historical suspense accounts would be presented to ARC in November.	
11.2	Regarding information presented to Post Masters in their customer accounts, TP advised these are settled centrally at the end of a trading period and that branches are expected to complete trading period accounting 12 times a year on a 5 week, 4 week, 4 week schedule at the end of each trading period. Letters are sent to Postmasters regarding their balance on the Monday following the scheduled branch balancing date, with a chaser sent the following week if no response is provided. It was noted that the letters have been updated since the Common Issues Judgment, and automatic deduction of monies has also ceased since the judgement, when no response is received from the Post Master. Revised processes and letters have been independently reviewed and approved by Norton Rose Fulbright as reflecting the requirements of the Common Issues Judgment. POL is currently completing a thorough review of its Loss Recovery policies and processes and is considering other opportunities, such as the use of Branch Hub, to allow Postmasters to monitor the balances on their customer account(s). The review will conclude in Q3 2020-21.	
11.3	Regarding trends, apart from in TP04 2020, the year on year balances settled centrally by branches has fallen year on year in each trading period over the last 20 months. The reduction in balances settled centrally is driven by a reduction in both the volume of branches settling balances centrally and the average value being settled centrally. the total level of declared losses across the network has also decreased, driven by an increase in the monitoring of branches, an increase in the support provided to branches and through more frequent earlier intervention for branches that are having operational issues.	
11.4	Regarding the review of further processes that could be identified as having a similar risks to stamps, the team had identified no further areas. As no further products/processes had been identified as at risk, TP advised that a high level review of the product portfolio would be conducted to identify key risk areas. This will include any products with specific process issues that may have the potential to cause product-related branch discrepancies, and where Postmasters may suffer detriment as a result.	

POL00423571

	These include as a minimum, processes for ATMs, Camelot (lottery and scratchcards), Paystation, Moneygram, Postal Orders, Foreign Exchange and Traveller's Cheques. The review will consider current and historical processes, where historical processes are known. The Committee remarked on the excellent progress made to improve data provided to Post Masters. The paper was **NOTED for onward submission to the ARC.**	
12.	**Policies for Approval:**	
12.1	The following policies were **NOTED for onward submission to the ARC:** • Procurement Policy • Contract Execution • Vulnerable Customer • Physical Security • HMRC Fit and Proper Standards	
12.2	BB presented the Procurement Policy. She explained that the Procurement policy (not reviewed since 2015) sets out the legal framework for Public Procurement Regulation under which POL operates as a public sector body. She noted that the regulations were published in 2015 and have not been altered since, save government notices on good practice. POL complies with these regulations. She set out that an Appendix A providing more detailed guidance on Sub Threshold awards has been drafted for discussion at RCC and ARC, as the regulation and guidance is much lighter and open to interpretation. Sub threshold awards is the area which is most often the subject of the recent Procurement Risk Exception Form (PREN) process. The object of this appendix is to establish the minimum operating standards relating to the risk management of procurement activity under PCR threshold values. It was noted the upper threshold is updated every two years to account for exchange rate variations between the UK and the Eurozone. A discussion took place on how the regulations are applied in practice and whether how "cross border interest" is interpreted drives significant additional effort. A decision on the interpretation of cross-border awards would be made by BF to avoid any internal confusion, and a review of how UKGI handle cross-border awards (and other similar organisations) would also be completed. The Committee recommended a pragmatic approach be taken, particularly with cross-border awards – whether more legal risk notes should be drafted in future, or a blanket approach to cross-border awards is taken and the resourcing impact and associated costs assessed.	
13.	**Review of draft Audit, Risk and Compliance Committee meeting agenda for 22 September 2020**	
13.1	The draft ARC agenda for 22 September was **NOTED**.	
14.	**Any other Business**	
	There was no other business.	

DRAFT

POL00423571



2.1

DRAFT

POL00423571

Post Office Limited
Risk & Compliance Committee
OPEN ACTIONS

No.	Meeting Date	Minute Reference	Action	Action Owner	Due Date	Comment
1	10/09/2020	3.6: GLO/Freedom of Information Requests/GDPR:	The team remains stretched responding to Historic Shortfall Scheme and related/linked FOI requests (186 open requests). Following receipt of 41 FOI enquiries considered vexatious from one journalist, 31,000 boxes of data (previously unknown) have now been identified in storage. These are being reviewed by legal, HSF and Peters and Peters and a separate paper for ARC will be prepared regarding this issue	Jonathan Hill	November RCC & ARC Meeting ~~September ARC Meeting~~	02/11/2020: This paper is being prepared and is on the RCC & ARC agendas under Data Governance. **Recommended for closure.**
2	10/09/2020	4. Pensions Assurance	The Committee requested a timetable and proposed quantum ahead of the ARC meeting, but noted that LC was due to meet the Chair of ARC separately to discuss this issue.	Lisa Cherry / Maxine Cross	Update @ January 2021 RCC Meeting ~~September~~	06/11/2020: Project Assurance Steerco has been created and will be meeting monthly following the initial meeting on 30th October 2020. Initial sets of reconstructed data were shared with the Trustee and Willis Towers Watson, POL's scheme advisors. Both wondered if the scheme rules had ben correctly interpreted which led to legal advisors for both POL and the Trustee reversing an earlier view about the application of the scheme rules. Data is being recalculated in accordance with the later view and is now expected to be completed in mid-November with POLs reviews expected to conclude at the end of November 2020. We intend to notify The Pension Regulator of this delay to the rectification timetable following their acknowledgement of our breach paper. In October, the POL Board was advised of a potential liabilities stemming from a provision in the Pension Administration Agreement. Our legal advisors think that the liabilities under this agreement will be capped at £300k (£150k per "event")
3	13/07/2020	7. Suspense Accounts	It was noted the review did not cover the historical operation of the suspense accounts, which the Chair requested be investigated.	Tim Perkins / Mark Underwood	September RCC Meeting	Update 30/10/2020: This paper has been prepared for the November RCC and will be presented by Mark Underwood. **Recommended for closure.** Previous Update: The work with KPMG remains on-going and a full report will be provided in November.
4	13/07/2020	3.5 Compliance Report	Fairness – the Telco team was asked to consider ways to reduce the number of 'vulnerable customers' and to revert to the Committee with a statement/plan for November.	Jonathan Hill / Meredith Sharples	November RCC & ARC Meeting	02/11/2020: This will be included in the Compliance Paper presented to the RCC & ARC. NOTE: there is an error in the minutes and the action should read: "*the Telco team was asked to consider ways to reduce the number of customers out of contract and to revert to the Committee with a statement/plan for November*."
5	06/05/2020	3.15 Combined Risk, Compliance and Audit Update: Internal Audit	Internal Audit reviews completed: The Fit & Proper policy was also being updated and LC was asked to ensure that HR were involved in this update	Lisa Cherry	January 2021 RCC Meeting	06/11/2020: This policy is due to be presented to the Committee in January 2021 and HR have discussed involvement with Ops and it was agreed the policy was to be owned by Ops. **Recommended for closure.** Previous: LC has spoken to JT and an update will be provided in September.

POL00423571

6	07/11/2019	10.6 - Money Laundering Reporting Officer (MLRO) Annual Report	BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC.	Sally Smith / Jonathan Hill	Update @ January 2021 RCC Meeting	02/11/2020: HMRC are still conducting any meetings - action to be updated at next meeting (January 2021). 09/07/2020: HMRC are not conducting meetings at present due to Covid, but Sally has chased.
7	07/11/2019	3.2 Supplier Contracts out of Governance	SSK – retail lead team decision required to ensure project does not stall.	Kathryn Sherratt / Nick Wade /Cathy Mayor / Marketing Additional: Angus MacDonald/Barbara Brannon/Lisa Watkins	Update @ January 2021 RCC (resolution by end of January 2021)	02/11/2020: SSK Procurement Project will now be formally closed and any future activity will sit under the Network Strategy workstream. Automation forms a clear part of this strategy and is fully backed by the Board. Network Strategy is due to go back to Board in January with an update on Automation and Technology (this includes SPM dependencies and route to procure). In relation to the existing estate the procurement team are investigating a PCR compliant route to maintain the current estate and potential procurement of new with a target resolution date of 29/01/2021. Previous: The SSK Procurement Project is on hold at present. This work will now form part of NEO Work Package 5, which is due to report to Board in June and July on Network Shape and Formats and Propositions respectively. NEO WP5 will return to Board in September with the Technology part of the work stream, the direction from which will form part of the Procurement. The project will return to PRB to resume work following the September Board.
8	07/11/2019	3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	Jeff Smyth / Marketing (David Enwright) Additional: Barbara Brannon	Update @ January 2021 RCC Meeting (contract by end of November)	02/11/2020: A compliant tender process has been run and the contract has been awarded to the incumbent provider, with operational costs reduced. Contracts are nearing finalisation with a target completion date of end November.
9	07/11/2019	5.3 Cyber Security	A major incident test be completed with findings reported to the Committee.	Tony Jowett	~~January 2020~~ 13/07/2020 (RCC Meeting)	02/11/2020: As per update to the September RCC - we will do a desktop exercise to bed in new processes in November and then in subsequent months use an external party Nettitude to conduct live tests. **Recommended for closure.** Previous: The test was scheduled for March but was interrupted by preparations for COVID – to be rescheduled. Update to be provided in Cyber Security update paper. July 2020 Update 06/05/2020: JS to provide an update in May.

POL00423571

Central Risk Dashboard

RCC & ARC

12 November 2020

Strictly Confidential

POL00423571

1. Summary

Summary

As @04/11 the Post Office has **492** open risks compared to **483** in 9/2020 (a net increase of **19**). So **20** new risks were articulated in 10/2020. Cumulatively we have seen 75 new risks raised ands 100 risks closed since 8/2020. Key points to note include:

- **21** new risks identified at the intermediate level – primarily over Brexit (Commercial), POI, FCC, Health & Safety.
- **100** risks closed (**64** net increase since last reporting) - primarily at local level (**96**). The majority are in Commercial (**35**) and Operations & Supply Chain (**32**).
- **COVID-19** risks have been assimilated within BAU risk management.
- **Brexit risks** have been uploaded onto the GRC tool, however agreement on their score and remediation plan is being proactively pursued by Central Risk
- **Risk Policy** and **Risk appetite/KRIs** statements revised - pending RCC/ARC approval
- **Strategy**: current risk profile under review as a result of the launch of a refreshed Post Office strategy. GE level risk survey being conducted in 11/2020.
- Historical Matters : Centra Risk in discussion with HMU and LCG regarding appropriate risk transfers

Central Risk Review

Central Risk seeing increasing levels of engagement from individual business units in managing the risks for which they are accountable (in their 1st line role).
Some areas of relative weakness remain. They include:

- Risk articulation: ongoing need to be clear on the cause, event and impact of the risk
- Alignment: Ensuring risks articulated elsewhere (such as in ARC and Board papers) are reflected and managed through RSA Archer
- Mitigations: sometimes need strengthening i.e. no mitigations at all, or not SMART (what, by who, by when)
- RAG ratings: need to ensure in some instances that risks have been rated in line with corporate standards
- Risk Assessment: need to carry out risk assessment on a monthly basis or before the expected response date

Risk Profile churn (cumulative)



Post Office Group: Risk weight[1] comparison (10/2020)



[1] Risk weight is calculated by taking individual risks (with the same impact and likelihood scores) and applying the same RAG rating to provide a cumulative total (i.e. 3 risks each with a 1:3 score have an overall risk weight of 9 (3x3). Risk weight is a more subtle measure of the risks being carried than a simple risk count.

Strictly Confidential

POL00423571

2. Enterprise Level: Summary

Summary

The Post Office has **15** active enterprise which provide the overall, thematic framework within which linked subsidiary intermediate and local risks sit.

Given their strategic nature enterprise risks do not see significant change in ratings month on month albeit 1 (Health & Safety) has been reduced to 4/4 to reflect the health and safety precautions in place in the business.

Central Risk have continued the work in the period to ensure that enterprise risk mitigation activity is shaped by the work and priorities of the linked intermediate and local risk rather than seen as standalone.

Legal, Operational and IT target ratings will be shaped followed by the planned approval of updated risk appetite statements and Key Risk Indicators expected in November.

Enterprise Risk Heat Map

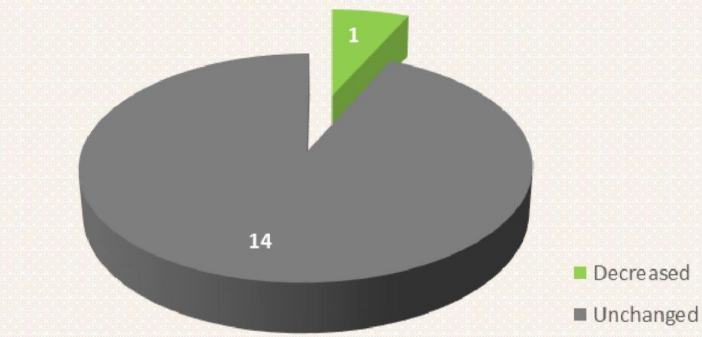


Key Risks

Key enterprise risks include:

- **Commercial:** Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market.
- **COVID 19:** Risk that the Post Office business employees and postmasters are adversely impacted by the spread of the COVID-19 virus and wider associated socio-economic activity.
- **Health & Safety**: Risk that the Post Office business and its staff are adversely impacted by health and safety event (e.g. pandemic), detrimental business activities and/or physical security.
- **Legal:** Risk the Post Office is unable to comply with legislative and regulatory changes.
- **Financial:** Risk that the Post Offices has insufficient funding and/or uncontrolled costs in the short-, medium and long-term.

Enterprise Risk rating change



Strictly Confidential

POL00423571

3. Enterprise Level: Key Risks

Risk #	Risk Owner	Enterprise Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Sept-20]	Latest Residual RAG (I/L) [Nov-20]	Trend	Actions/Mitigations	Target RAG (I/L)
12	Owen Woodley	**Commercial:** Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market.	(4/3)	(4/4)	(4/4)	⇨	• PO Strategic review - Commercial strategic review of what does the business look like after of Covid 19 currently underway to identify what Markets are critical for Post Office and the supporting operational functions and dependencies to support this, including key systems, staff, third parties, polices and operational hub. Proposed future Commercial structure and new purpose announced in 9/2020; In 10/2020, GE-1 roles level and GE-2 roles (for Customer Experience) have been defined. The remainder of GE-2 level will work on a 'lift and shift' reporting line basis from 11/2020. • Commercial Policy & Procedure review - Undertake policies and procedures review to ensure they remain adaptive and flexible to long-term (12/2020).	(3/3)
84	Al Cameron	**COVID 19:** Risk that the Post Office business employees and postmasters are adversely impacted by the spread of the COVID-19 virus and wider associated socio-economic activity.	(4/4)	(4/4)	(4/4)	⇨	• Government guidelines – followed and shared to guidelines of maintaining minimum distance (2m) between customers/staff. • PPE - issued and all DMB branches and depots are Covid Secure. • Vulnerable people - Extremely clinically vulnerable people shield during national lockdown and on return to workplace, undertake an individual risk assessment and adjustments are agreed where appropriate.	(3/3)
19	Al Cameron	**Health and Safety:** Risk that the Post Office business and its staff are adversely impacted by health and safety event (e.g. pandemic), detrimental business activities and/or physical security.	(4/5)	(4/5)	(4/4)	⇩	• New COVID-19 Secure risk assessments - completed and updated for every DMB • Individual risk assessments - completed for vulnerable people. • Controls - monitored closely and evidence of compliance received. • New Bespoke risk assessments - completed for Tablet transaction and all RAs are backed up with advice and guidance issued to Managers and Colleagues. • Support Centres - unoccupied except for exceptional at risk workers and risk assessments completed and COVID secure and safe working practices implemented.	tbc
18	Ben Foat	**Legal:** Risk the Post Office is unable to comply with legislative and regulatory changes.	(5/3)	(5/3)	(5/3)	⇨	• Group Litigation Fallout - There is a GLO programme in place which is managing the current position including the ongoing litigation and increase in the number of postmasters impacted. • Project Starling - [redacted] Trial listed for 6/2021. [redacted]	(3/2)
20	Al Cameron	**Financial:** Risk that the Post Offices has insufficient funding and/or uncontrolled costs in the short-, medium and long-term.	(5/3)	(5/3)	(5/3)	⇨	• PO Strategic review (Project NEO) - Commercial strategic review of likely post-COVID-19 environment to determine optimal operating requirements and associated required funding. • Cashflow monitoring - weekly budgeting implemented; industry cashflow impacts of COVID pandemic being monitored.	tbc

POL00423571

4. Intermediate Level: Summary

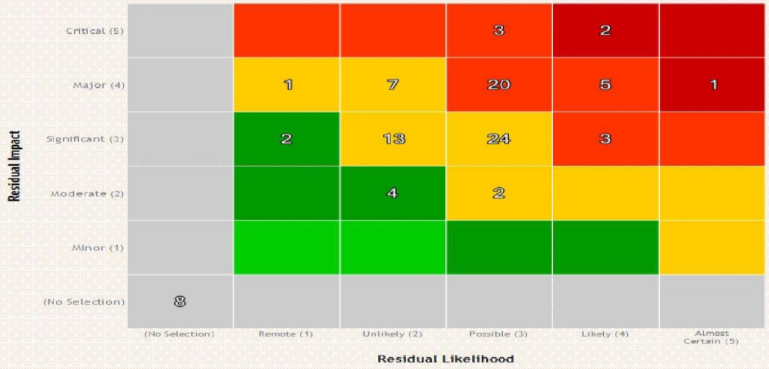
Summary

The Post Office has **95** intermediate risks of which **3** are rated as Critical, **31** Very High and **47** high.

The ratings of 73% of these risks remain unchanged since the last reporting period, while 17% has seen an increase and 10% a decrease. Central Risk are requesting an urgent update of Brexit and COVID-19 risks to agree them and their remediation plan by mid-November. The COVID-19 risks will form part of the weekly report to the GE sub-group.

28 intermediate risks are in the Commercial space. These include new risks for POI and Brexit risks.
4 new risks have been identified in the Health & Safety space and **5** around Financial Crime and Data Protection.

Intermediate Risk Heat Map

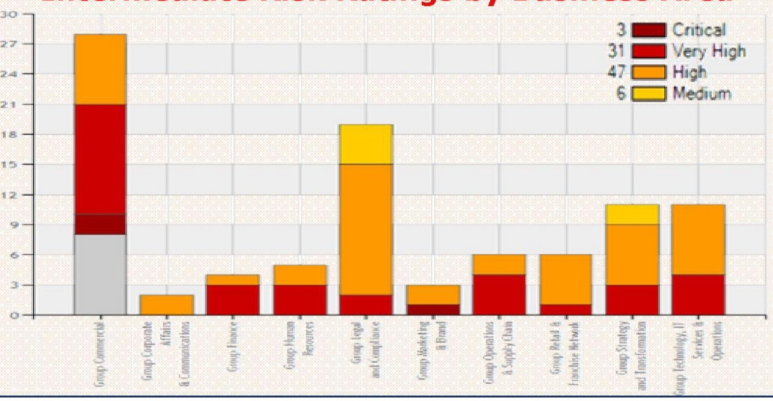


Key Risks

Key risks include;

- Government Services: Risk the Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) may reduce over the short-, medium- and long-term.
- Telco Dependency: Risk Post Office has limited influence on Fujitsu's T&C's (or ability to exit) therefore undermining performance and change affordability.
- Customer Demand: Risk existing and emerging requirements of Post Office (new and existing) customers across the various sectors are not met such that customer demand declines rapidly in a 3-10 year timescale and the Post Office is unable to change cost base ahead of curve resulting
- Digital Income: Risk the on-line products and services generate a reduced income level compared to comparable physical products and services.
- Financial COVID 19: Risk Post Office is unable to manage its finances in accordance with requirements and financial constraints.

Intermediate Risk Ratings by Business Area



POL00423571

5. Intermediate Level: Key Risks

Risk #	GE Risk Owner	Intermediate Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Sept-20]	Latest Residual RAG (I/L) [Nov-20]	Trend	Actions/Mitigations	Target RAG (I/L)
70	Owen Woodley	**Government Services:** Risk the Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) may reduce over the short-, medium- and long-term.	(5/4)	(5/4)	(5/4)	⇨	• Remediation plan still needs to be agreed. • Reviewing a faster roll out of the tablet services to ensure ready for travel bounce-back period. • Discussing with marketing an awareness campaign to put PO services front of mind, emphasising ease and certainty that comes through transacting with the Post Office. • Regular meetings with Government Departments in the role PO can play.	tbc
53	Owen Woodley	**Telco Dependency:** Risk Post Office has limited influence on Fujitsu's T&C's (or ability to exit) therefore undermining performance and change affordability.	(4/5)	(4/5)	(4/5)	⇨	• Remediation plan has not yet been updated as requested (expired on 1/9/20). • Fujitsu contract ended in August 2020 and tendering process has concluded with an alternative supplier Talk Talk. The potential impact of this Fujitsu may not be proactive in ensuring they are meeting their contractual obligations and cause a risk a breakdown in the relationship. • Since the last review there has been a further incident in respect of Telco - Breach of regulatory communications re FJT P1 communications which will result in a full investigation from Ofcom resulting in a fine. An action plan to address the incident is in place but no to address the wider risk.	2/1
48	Emma Springham – tbc	**Customer Demand:** Risk the existing and emerging requirements of Post Office (new and existing) customers across the various sectors are not met.	(5/4)	(5/4)	(5/4)	⇨	• Increase investment in insights and the insights team to understand the customer needs better and develop products and proposition that align to customers – this decision that is needed at GE level. • Increase brand spend so PO awareness and consideration is high amongst new and existing customers and that they feel PO is a brand for them.	3/2
64	Owen Woodley	**Digital Income:** Risk the on-line products and services generate a reduced income level compared to comparable physical products and services.	(5/4)	(4/4)	(4/4)	⇨	• Digital & Innovation (D&I) team has established an agile way of concurrent deployment by having stood up 2 sprint teams (ACE and FARGO) and having installed a daily drum beat of stand-ups with the cross functional teams. FARGO is an internal capability and ACE is an external capability which can be scaled up at any time (with Accenture). • There is a weekly D&I governance meeting addressing demand and capacity which is headed by a permanent role within D&I.	3/2
89	Al Cameron	**Financial COVID 19**: Risk the Post Office is unable to manage its finances in accordance with requirements and financial constraints.	(4/5)	(4/4)	(4/4)	⇨	• Monitor industry cashflow impacts. • Weekly budgeting.	tbc

Strictly Confidential

POL00423571

6. Local Level: Summary

Summary

The Post Office has undertaken significant work in recent months to ensure all local risks are uploaded onto the GRC tool and linked directly to higher level enterprise and intermediate risk levels to provide an overall, risk profile across specific themes.

The current data shows (as at 4/11/20) we have **457** open Local Level risks. This is a **+71** net increase since 8/2020 (**54** new risks raised and **96** closed). The bulk of these low level risks have been categorised as Commercial (**61**), Operational (**63**) and Legal (**91**). The latter cover risks around potential non-compliance across various regulations (AML, ABC, vehicle safety, environment etc). There has also been **52** Security local risks and **32** Technology risks. Commercial has reported 1 new 'Critical' risk by the Telco team. This concerns a breach of regulatory communications following the FJT P1 communications incident which could result in an Ofcom investigation. A remediation plan is in progress to fully mitigate this risk.

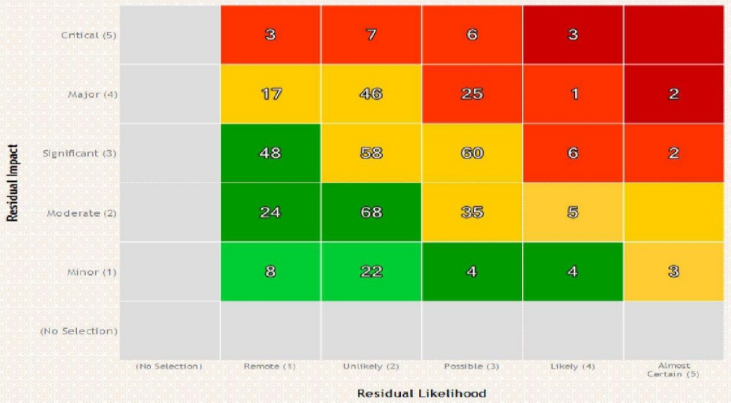
Central Risk are continuing to proactively liaise with Business Risk Leads to ensure local risks are correctly articulated, rated and their remediation updated, following the new proposed PO Structure and Purpose. Target ratings for most risks await the outcome of the risk appetite and KRI work.

Key Risks

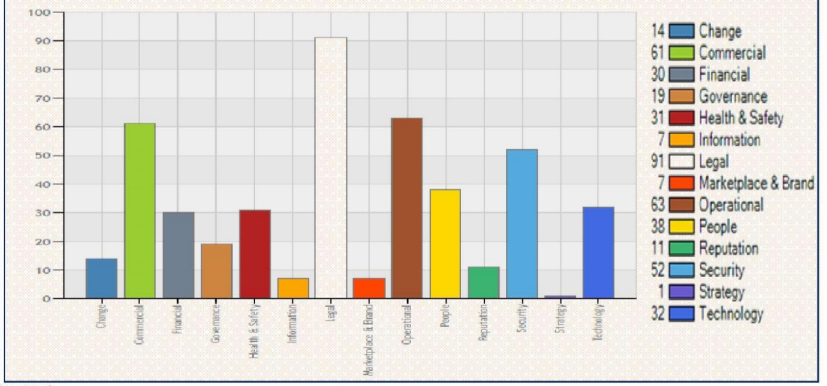
There are 5 Local Level risks whose current rating is Critical (20) namely:

- Industrial Action: Risk the Post Office Commercial proposition is unattractive because existing products are too complex or confusing, new product are cost ineffective, unattractive to the market and/or unable to be scaled. Key mitigation include refreshed IR Framework, direct comms to Field teams and employees, and regular review of IA contingency plans.
- Health and Safety Breach - Branch Network and Mental and physical health and safety: Risk of harm or breach of regulatory requirements and risks through crime such as violence and hate crime. Physical safety and associated effects continues to be a key concern for the business. This could be exacerbated by the combination of coronavirus measures and Brexit disruption, and contingency plans are in place for ensuring branches remained stocked but do not hold unnecessary cash.
- External Fraud: Risk of fraud being carried out by external parties.
- Telco - Breach of regulatory communications: Risk the FJT P1 communications incident will result in a full investigation from Ofcom resulting in a fine.

Local Risks Heat Map



Local Risks by Category



POL00423571

7. Local Level: Key Risks

Risk #	GE Risk Owner	Local Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Sept-20]	Latest Residual RAG (I/L) [Nov-20]	Trend	Actions/Mitigations	Target RAG (I/L)
183	Amanda Jones	**Industrial action - Directly Managed Branches (DMB):** Risk of Industrial action because of proposed changes to the DMB network.	(5/4)	(4/5)	(4/5)	⇨	• IR Framework • Direct comms to employees • Regular review of IA contingency plans • Programme management held within DMB network. • Field teams kept up to date with plans and briefed on how programme activity will impact on the wider network	tbc
178	Amanda Jones	**Health and Safety Breach - Branch Network:** Risk of harm or breach of regulatory requirements.	(5/4)	(5/4)	(5/4)	⇨	• Develop greater awareness of safety responsibilities across whole Network • Implement new Accident investigation tool in DMBs, additional workshops for PiCs in DMBs in 20/21 to support launch of new Site Log Books and ensure all Managers and colleagues have completed all H&S training modules • Share best practice with Postmasters.	tbc
457	Al Cameron	**Mental and physical health and safety:** Risks through crime such as violence and hate crime	(5/4)	(5/4)	(5/4)	⇨	• Hate Crime campaign • Safety video on Branch Hub • Increasing the number of Health Check calls to branches	tbc
424	Al Cameron	**External Fraud:** Risk of fraud being carried out by external parties.	(5/4)	(5/4)	(5/4)	⇨	• Monitor emerging fraud risks (Nov 2020) • Branch holdings to be capped at £250k (Supply Chain)	tbc
510	Owen Woodley	**Telco - Breach of regulatory communications:** There is a risk the FJT P1 communications incident will result in a full investigation from Ofcom resulting in a fine.	(4/5)	N/A	(4/5)	New	• Outbound and inbound communications. • Weekly meetings held with FJT to track actions, ensure deadlines are met and minutes are documented. • No end date defined for inbound comms.	tbc

Strictly Confidential

POL00423571

8. Change Risks[1]

Themes	Previous Month's RAG Status	Current Month's RAG Status	Summary Points
Overall	Red	Amber	Overall RAG status changed from Red to Amber due to reduced 20-21 investment forecast, though benefits remains under budget. Continue to prioritise, delaying projects to accommodate current litigation position. Also considering impacts on security headroom. Historical Matters Business Unit will operate as a separate governance process. A simplified change portfolio structure has also been introduced.
Benefits	Red	Red	P6 year to date Change benefits were £35.4m, 6+6 forecast shows benefits £26m below full year budget mainly driven by the decision to delay and reduce the scope of tranche 1 People Programme, reclassification of Blackhawk Giftcard benefits, removal of benefits associated with the Agents Remuneration Review, market condition impacts and migration delays on Insurance projects (further impacted by CV19) and agreed delay to DMB activity.
Investment	Red	Amber	Year to date at P6 Change budget underspent by £23.8m. Mainly driven by decisions to delay organisational and DMB changes. The 6+6 forecast reduced the FY20-21 investment to £169m vs budget of £159m. Material changes driving reduction are latest assumptions of timing of settlements under HMBU and revised assumptions on DMB programme.
Risk	Amber	Amber	The number of Gold & Platinum projects reporting a Red risk status remains at 2.
Delivery	Amber	Amber	Four gold/platinum projects closed in period as well as Paystation Refresh completing delivery

Portfolio	Previous Month's RAG Status	Current Month's RAG Status	Summary Points
Banking, Payments & Other	Amber	Amber	ATM Banking Strategy and Paystation Refresh both reporting green, with Payzone and British Gas, reporting red in some areas. British Gas in closure
IT Platform Enablement	Amber	Amber	4 of 7 projects reporting green overall. PCI reporting red on cost and delivery. Fujitsu negotiations (Everest) is currently in the closure process
Mails, Travel, FS & Other	Amber	Amber	Telco Fujitsu Extension reporting green, Telco Strategy reporting amber and Identity Services and Mails strategy both reporting red in some areas. Identity Services in closure
Organisational Effectiveness	Amber	Amber	All People programmes reporting green, though Project Assurance reporting red
Postmaster & Network	Green	Green	4 of the 6 projects reporting green with DMB and Fit & Proper both reporting amber
Shared Services	Green	Green	Starling and Source to Settle both reporting green

[1] UKGI monthly report (P6 – 7/2020)

POL00423571

1. Risk Policy

Policy GE Sponsor	Policy Owner	Contact Details	Review History
Alisdair Cameron	Mark Baldock	GRO	November 2019

1.1 Purpose and Principles

The Risk Policy is organised around 3 themes: Risk Governance, Strategy and Protocols. The Policy outlines the minimum control standards that apply to each of these themes. It is supported by a Risk Management Framework, which provides additional detail and guidance to support the identification and management of risk across the organisation.

The principles are based on ISO:31000 (Risk Management–Principles and Guidelines)[1]. They also have regard to the UK Corporate Governance Code (Guidance on Risk Management, Internal Control and Related Financial and Business Reporting). The principles include:

a) Risk management is fundamental to how Post Office is directed, managed and controlled at all levels
b) Risk must be embedded in all activities. Its underlying risk culture and approach is key to effective decision making
c) All material risks must be identified, measured, monitored, managed and reported
d) Risk management processes must be aligned and integrated with the delivery of Post Office's strategy
e) Risk management must follow a consistent, transparent and auditable methodology
f) Risk reporting must allow for the effective review, challenge and monitoring of risk exposure against Post Office's approved risk appetites
g) Risk Governance must adhere to the industry standard '3 lines of defence' model.

1.2 Key definition

The Policy definition of 'risk' is based on the ISO 31000 definition namely the effect of uncertainty on the Post Office achieving its strategic objectives. That effect may be positive, negative or a deviation from the expected. Risks are described in terms of causes, potential events and their consequences.

1.3 Application

This Policy applies to Post Office Limited (excluding Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payment Limited although they will have regard to it) and to all Post Office employees, contractors and business operations.

1.4 Risk Governance

Post Office's Risk Governance arrangements are concerned with how risks are managed and reported within the organisation. Risk Governance includes:

- Structure: The Post Office risk management structure consists of the Board, ARC, RCC and Group Executive (GE)
- Roles and Responsibilities: Post Office follows the industry standard '3 lines of defence' model with regard to risk management governance, compliance and oversight
- Risk Reporting: Post Office has in place a reporting cycle for enterprise, intermediate and local risks. Specific dashboard reports are produced for each GE Business Unit and the corporate GE every month and the RCC/ARC every 2 months
- Escalation: Where the Risk Owner has insufficient authority to effectively manage the risk, they should escalate the risk to their relevant GE member, or equivalent senior leader.

[1] ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization.

POL00423571

1.5 Risk Strategy

The Post Office's Risk Strategy is concerned with specific risk policies and framework, appetite and attitude to risk, the techniques by which Post Office assess risks as well as the key priorities in any given year. Risk Strategy includes:

- Strategic objectives: This Policy and the supporting risk management framework is focused on managing the risks and opportunities of Post Office associated with its strategic purpose of 'We're here, in person, for the people who rely on us'
- Risk Appetite & Key Risk Indicators (KRIs): The Post Office's '3 lines of defence' risk management structure oversees Post Office's risk appetite and KRIs. Post Office assess risk appetite against a 5-tiered scale
- Exceptions: On occasions Post Office may need to accept risks that are outside of approved appetite or outside of existing procedures. Such circumstances must be exceptional, time-limited, formally documented (through a Risk Exception Note) and approved by the relevant GE member.

1.6 Risk Protocols

The Post Office Risk Protocols are the guidelines provided to the organisation for the management of risk. Risk Protocols include:

- Risk Management Process: The Post Office Risk Management Process is consistent with the principles of ISO: 31000 and it has a number of sequential components including Establishing the Context, Risk Assessment, Monitor & Review and Consultation
- Harm table: The Post Office corporate HARM table describes the risk impact/likelihood scales (on a standard 1-5 scale) which must be applied
- Risk Hierarchy and Classification: Post Office has a three-level risk hierarchy: Enterprise, Intermediate and Local risks. The Post Office risks are allocated one of fourteen categories consistent with those advocated by HM Government's 'Orange Book'
- Risk articulation: All risks across the risk hierarchy must be expressed in terms of their cause(s), the risk event itself, and their impact.

1.7 Minimum Control Standards

Post Office has a number of minimum control standards which apply to the management of its risks. Below is an example of the relationships between the risk area and the required minimum control standards:

Risk Policy Area	Risk Description	Minimum Control Standards	Accountability	Assessment Timing
Risk Governance (Roles & Responsibilities)	Risk that the GE and Post Office Groups do not perform their 1st line function and fail to proactively identify, assess, own and manage their risks and/or maintain their associated internal control measures	**Detective control**: Monthly, Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) review and update their risks (including current residual risk score, mitigating actions, target risk rating etc.) to the corporate GRC tool.	Risk Leads Risk Owners	Monthly

POL00423571

GROUP POLICIES
RISK POLICY

Version 1.1 – Final - Draft

DRAFT

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

POL00423571

1. Overview 4
1.1. Introduction by the Policy Owner 4
1.2. Purpose 4
1.3. Principles 5
1.4. Application 5
1.5. Compliance 5
2. Risk Governance 6
2.1. Structure 6
2.2. Roles and Responsibilities 6
2.3. Risk Reporting 6
2.4. Escalation 7
2.5. Transfer 7
3. Risk Strategy 8
3.1. Strategic Objectives 8
3.2. Risk Appetite & Key Risk Indicators (KRIs) 8
3.3. Exceptions 9
4. Risk Protocols 10
4.1. Risk Management Process 10
4.2. Harm Table 11
4.3. Risk Hierarchy and Classification 11
4.4. Risk Articulation 12
4.5. Governance, Risk & Compliance (GRC) tool 13
4.6. Incidents 13
5. Minimum Control Standards 14
6. Linked material & Contacts 17
6.1. Linked material 17
6.2. Contacts 17
7. Governance 18
8. Definitions 19
9. Appendices 20
9.1. Risk Appetite scale 20

DRAFT

POL00423571

9.2. HARM Table 21
10. Control 22
10.1. Policy Version 22
10.2. Policy Approval 22
10.3. Company Details 22

DRAFT

1. Overview

1.1. Introduction by the Policy Owner

The risk landscape in which Post Office operates is volatile, uncertain and complex, with increasing demands from its customers and greater scrutiny from regulators, legislators and Government. This will continue.

This is why Post Office must focus relentlessly on actively monitoring and strengthening its approach to risk management and promoting a consistent risk-intelligent culture.

Failure to effectively manage its risks will adversely impact Post Office's ability to deliver its business strategy, will undermine the protection and preservation of its reputation and brand, and the delivery of consistent, high-quality services.

In doing so Post Office acknowledges that risk exists in everything it does. So everyone in the organisation has a duty of care to manage these risks. However, risk management is as much about exploiting opportunities as it is about managing threats. Given this Post Office will inevitably take a certain amount of risk in order to achieve its strategic objectives.

This Risk Policy (with its clear principles and mandatory minimum control standards) is an important tool in managing risks efficiently and effectively.

1.2. Purpose

This Policy is organised around 3 themes:

- **Risk Governance**: This focuses on how Post Office risk management activity is **organised**. It describes (i) the relevant Committees (and their respective roles with regard to risk and how they interact), (ii) the '3 lines of defence' risk management model (and where accountability and responsibility are placed within it) and, (iii) the criteria by which risks should be escalated to provide the requisite oversight;
- **Risk Strategy**: This focuses on Post Office's overall **approach** to risk management. It describes how risk management activities are aligned, the level of risk maturity being sought and the level of risk exposure (appetite) that is acceptable; and,
- **Risk Protocols**: This defines the risk management **activities** that must be undertaken, how they will be undertaken and their frequency.

The Policy also outlines the **minimum control standards** that apply to each of these themes.

It is supported by a Risk Management Framework (a series of separate but interlinked documents) which provides additional detail and practical guidance to support the consistent and robust identification and management of risk and opportunities across the organisation.

This Policy, the supporting Framework and other material is accessible on Post Office's Central Risk intranet site.

POL00423571

1.3. Principles

The Post Office's Risk Policy principles are based on ISO:31000 (Risk Management–Principles and Guidelines).[1] They also have regard to the UK Corporate Governance Code (Guidance on Risk Management, Internal Control and Related Financial and Business Reporting)[2]. There are 7 principles:

1. Risk management is fundamental to how Post Office is directed, managed and controlled at all levels;
2. Risk must be embedded in all Post Office activities. Its underlying risk culture and approach is key to effective decision making;
3. All material risks must be identified, measured, monitored, managed and reported on a continuous basis at an individual and aggregate level;
4. Risk management processes must be aligned and integrated with the delivery of Post Office's strategy and in such a way that supports an enterprise wide approach;
5. Risk management must follow a consistent, transparent and auditable methodology and proactively recognise external factors, opportunities, and uncertainties;
6. Risk reporting must allow for the effective review, challenge and monitoring of risk exposure against Post Office's approved risk appetites; and,
7. Risk Governance must adhere to the industry standard '3 lines of defence' model to ensure clear accountability and appropriate segregation of duties.

1.4. Application

This Policy applies to Post Office Limited[3] (excluding Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payment Limited although they will have regard to it) and to all Post Office employees[4], contractors and business operations.

1.5. Compliance

This Policy is mandatory for all Post Office employees, contractors and business operations and applies wherever in the world Post Office Limited's business is undertaken. All Post Office third parties who do business with the Group (including consultants, suppliers and business partners) will be required to agree contractually to this Policy or have their own equivalent Policy.

Where significant non-compliance with the Risk Policy is identified the matter must be referred to the Chief Finance Officer and the Head of Risk.

---

[1] ISO 31000 is a family of standards relating to risk management codified by the International Organization for Standardization.

[2] The UK Corporate Governance code, (formerly known as the Combined Code) is part of UK company law with a set of principles of good corporate governance aimed at companies listed on the London Stock Exchange. It is overseen by the Financial Reporting Council.

[3] Post Office Limited is wholly owned by the Department for Business, Energy and Industrial Strategy (BEIS). Its business consists of the core products and services provided by Post Office Group (mails, telecoms, government services (including identity & licences) and retail), as well as selling the services of Group Companies and joint ventures (Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payments Limited). However, this Policy is not applicable to Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payment Limited.

[4] In this Policy "employee" and "staff" means all persons working for the Group (excluding Post Office Insurance, First Rate Exchange Services Limited and Payzone Bill Payment Limited) or on its behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.

POL00423571

2. Risk Governance

Post Office's Risk Governance arrangements are concerned with how risks are managed and reported within the organisation.

2.1. Structure

The Post Office risk management structure consists of the:

- **Board**[5], informed and advised by the Audit, Risk & Compliance (ARC). They have overall accountability for the assessment and management of risk, taking a strategic view of the risks faced by Post Office;
- **ARC**[6]. They support the Board in its assessment and management of risks. The ARC reviews Post Office's risk policy, risk appetite and attitude to risk to ensure these are appropriately defined and communicated so that parameters and expectations are understood; and,
- **Group Executive (GE)**[7]. The GE, led by the Chief Executive, has operational responsibility for Post Office risk management and systems of internal control.

2.2. Roles and Responsibilities

Post Office follows the industry standard '3 lines of defence' model with regard to risk management governance, compliance and oversight. This means:

- The **GE and Post Office Groups** (and their subsidiary business units) perform the **1st line function**. They are accountable for identifying, assessing, owning and manage their risks. They are also accountable for the design, implementation and maintenance of the associated internal control measures;
- The **Central Risk** team perform the **2nd line function**. They oversee the corporate approach to risk management. This involves defining and implementing risk standards, policies, procedures and guidance. They also assist the 1st line function in the management of their risks in line with good practice as well as monitor compliance and effectiveness. Furthermore, they are accountable for reporting to the Board, ARC and GE on Post Office risk performance as well as advising on emerging risks and changing risk scenarios; and,
- **Internal Audit**, who operate independently of 1st and 2nd Line functions, are the **3rd Line**. They provide an independent evaluation of the adequacy and effectiveness of Post Office's framework of governance, risk management and control.

2.3. Risk Reporting

All Post Office risks must be monitored, reviewed and recorded regularly to determine whether, or not, the corporate risk profile has changed and to gain

---

[5] The Board is collectively responsible for setting Post Office's strategic direction and primary business objectives. It establishes a robust governance framework and ensures that the Company has financial and human resources required to achieve its agreed objectives. It is chaired by a non-Executive Director.

[6]. The ARC is a Committee of the Board from which it derives its authority. It provides oversight of Post Office's Group's risk management systems, operational controls and key systems, including monitoring exposures to the Group Risk Appetite.

[7] The GE is a Committee of Post Office senior management responsible for day to day Post Office operational management.

POL00423571

assurance that corporate risk management rules and procedures are effective. Such regular (and incremental) reporting has a number of benefits including:

- ensuring responses are effective and efficient;
- building up knowledge to improve risk identification and analysis;
- providing a better link between risks and objectives, key dependencies, core processes and stakeholder expectations;
- detecting and preparing for changes and trends in existing risks, including the extent to which risks are aligned with approved appetite;
- identifying and preparing for new and emerging risks; and,
- identifying good risk management practice, building on it and disseminating it to other parts of the organisation.

Post Office has in place a reporting cycle for enterprise, intermediate and local risks. Specific dashboard reports are produced for each GE Business Unit and the corporate GE every month and the RCC/ARC every 2 months. These reports include (but are not limited to) information on risks trends, compliance levels and associated actions. The data is taken directly from Post Office's Governance, Risk & Compliance tool which provides a 'single source of truth'.

2.4. Escalation

Post Office has a 3 tier risk hierarchy (see Section 4.3) with each risk having a designated Risk Owner accountable for proactively managing their risks to within an approved level of appetite.

Where the Risk Owner has insufficient authority to effectively manage the risk, they should escalate the risk to their relevant GE member, or equivalent senior leader. This should be done in circumstances where:

- treatment of the risk requires decisions/actions beyond what the Risk Owner is authorised to decide and/or there are commercial constraints;
- the risk may impact multiple business areas and/or addressing the risk requires action by multiple stakeholders;
- addressing the risk requires corporate changes; or,
- grievances from stakeholders have been received to which the Risk Owner cannot impartially and/or effectively respond.

When a risk is escalated, the Risk Owner must provide the receiving manager with complete information about the risk to enable the latter to act appropriately. Risk ownership can only be transferred when a risk has been escalated and accepted. Escalation does not require the impact and/or likelihood rating of a risk to be 'artificially' inflated to give it visibility.

2.5. Transfer

Risk ownership can be transferred where the risk has:

- been escalated;
- to be reallocated within the organisation due to internal restructure; or,
- has changed and it needs to be reassigned.

When a risk is transferred, the Risk Owner must provide the new owner with complete information about the risk to enable them to manage the risk appropriately. Risk ownership can only be transferred when a risk has been accepted by the new Risk Owner.

3. Risk Strategy

The Post Office's Risk Strategy is concerned with specific risk policies and framework, appetite and attitude to risk, the techniques by which Post Office assess risks as well as the key priorities in any given year.

3.1. Strategic Objectives

This Policy and the supporting risk management framework is focused on managing the risks and opportunities of Post Office associated with its strategic purpose of 'We're here, in person, for the people who rely on us.' Such focus increases the probability of success (and reduces the likelihood of failure) in:

- supporting Post Office Postmasters (i.e. making sure that Postmasters feel that they have a role in shaping the business);
- building a fit for purpose network (i.e. having the right branches in the right place); and,
- focusing relentlessly on Post Office core strengths and customers (i.e. defending and growing main products and services that are so critical to Post Office income.

3.2. Risk Appetite[8] & Key Risk Indicators (KRIs)[9]

Post Office has in a place a series of risk appetite statements and KRIs to:

- allow the Board, GE and ARC to understand the organisation's aggregated and interlinked levels of risk to determine acceptability or not;
- provide further assurance that the strategic objectives will be secured and early warning where these are under threat;
- allow the business to focus limited resource to manage risks outside of tolerance and tolerate risks which lie within the thresholds;
- support management in making decisions with an understanding of the degree to which the business is exposed to the consequences of a risk event; and,
- flex and adapt to the changing business environment.

The Post Office's approach is based on industry-standard principles[10] namely:

- Scope: Risk appetite/KRIs are primarily articulated at the enterprise risk level and guide/shape the management of linked (but subsidiary) intermediate and local risks;
- Complex: Risk appetites/KRIs are complex given that excessive simplicity, while superficially attractive, is counter-productive;
- Measurable: Risk appetites/KRIs are measurable so are based on relevant, accurate and readily available existing data;
- Flexible: They are not single, fixed concepts. There will be different (and tailored) appetites for different enterprise risks; and,

[8] Risk Appetite is the amount of overall risk an organisation is willing to pursue (or retain) to achieve the relevant strategic objective. It is a qualitative assessment generally made at enterprise risk level.
[9] Key Risk Indicators (KRIs) are measures put in place to show the underlying trend of specific risks. KRIs are predictive. They are a set of 'guide rails' to provide context within which individual risk impact and likelihood ratings can be considered. KRIs are a quantitative assessment again generally made at enterprise risk level.
[10] Institute of Risk Management: Risk Appetite & Tolerance Guidance paper – 9/2011. Gartner: Ignition Guide to Drafting and Operationalizing Risk Appetite – 2/2020

POL00423571

- Manageable: The approach considers Post Office's risk management capability and the organisation's willingness and capacity for taking risks and level of maturity in managing them.

The Post Office's '3 lines of defence' risk management oversee its risk appetite and KRIs as follows:

1st Line	Board/ARC[11]	• Approve all final draft Risk Appetite Statements and associated KRIs. • Request, as necessary, the Group Executive commission work to articulate additional Risk Appetite Statements/KRIs • Seek assurance Post Office is adhering to approved Risk Appetite Statements/KRI thresholds
	Group Executive	• Effectively and clearly communicate goals and objectives, strategy, achievement metrics, and relevant time periods for pursuing the objectives related to developing risk appetite statements. • Set the Risk Appetites and approved tolerance levels that ensure enough risk is being taken to ensure Post Office strategic objectives are met • Secure Group Command consensus on statements and approach. • Commission revisions of Risk Appetite Statements and KRIs as needed.
	Group and individual Business Units	• Validate or raise concerns about the ongoing viability of existing Risk Appetite Statements approved by the GE /Board • Monitor existing KRIs to determine adherence to Risk Appetite Statements that apply to the Group
2nd Line	Central Risk	• Produce Post Office corporate policy/standards for Risk Appetite and KRIs • Develop (in discussion with 1st Line) initial set of corporate Risk Appetite Statements and KRIs • Facilitate ongoing development of new (and enhancements to existing) Risk Appetite Statements and KRIs • Provide assurance of 1st Line compliance with standards in this area • Escalate areas of non-compliance to Group Executive and Board/ARC
3rd Line	Internal Audit	• Provide, as part of its agreed Audit plan, an independent and objective evaluation of the adequacy and effectiveness of the risk management and control, making recommendations for improvement • Report to RCC/ARC on its findings, particularly around areas of non-compliance

Post Office assess risk appetite against a 5-tiered scale (see section 9.1).

3.3. Exceptions

On occasions Post Office may need to accept risks that are outside of approved appetite or outside of existing procedures.

Such circumstances must be exceptional, time-limited, formally documented (through a Risk Exception Note) and approved by the relevant GE member.

Central Risk report regularly on all open Risk Exception Notes to the GE and ARC. They are accountable for assuring the relevant business unit are proactively managing in a timely fashion and the necessary mitigating actions are being taken to close the exception.

[11] After Initial RCC discussion and approval

POL00423571

4. Risk Protocols

The Post Office Risk Protocols are the guidelines provided to the organisation for the management of risk. These include detailed rules and procedures, how risks are classified, as well as the risk management methodologies, tools and techniques used.

4.1. Risk Management Process

The Post Office Risk Management Process is consistent with the principles of ISO: 31000.

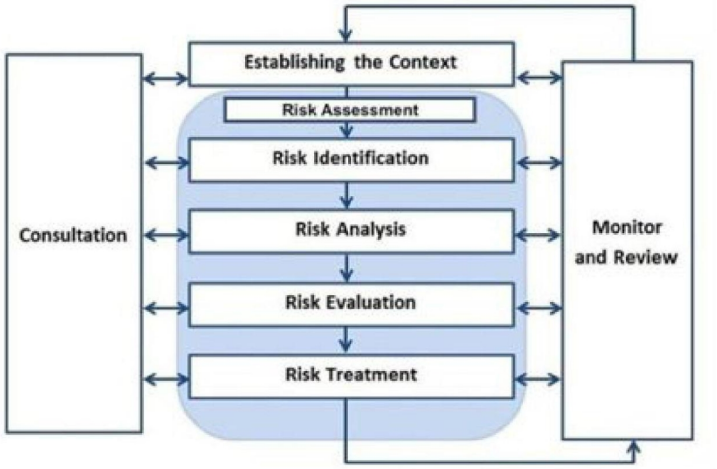


Figure 1: Post Office Risk Management process

It has a number of sequential components:

1. **Establishing the Context**: Post Office risks should be understood in the context of the organisation itself, the activities it undertakes and the range of skills and capabilities available to it. Consideration must also be given to the environment in which Post Office operates, its external stakeholders and their expectations.
2. **Risk Assessment**: This is the means by with which Post Office should evaluate and prioritise the risks it faces through:
   a) Risk Identification: Techniques by which Post Office identifies all the risks its faces be they existing, new or emerging
   b) Risk Analysis: whereby each risk is assessed in terms of its potential impact and likelihood (see Section 3.2) and its relationship to the associated approved appetite (see Section 0)
   c) Risk Evaluation: a risk profile is produced providing a significance rating to each risk and therefore a tool for prioritising treatment efforts;
   d) Risk Treatment: implementation of actions to respond to risks including decisions on whether to tolerate, treat, transfer or terminate
3. **Monitor & Review:**
   This is focused on (a) reacting to early warning indicators of the need to make interventions, (b) reviewing emerging risks and opportunities, (c) reviewing whether risks owners are implementing the responses for which

they are accountable and, (d) reporting on the success (or otherwise) of the interventions to date and whether additional activity is required.

4. **Consultation:** This should ensure that (a) appropriate decisions and actions are taken to respond appropriately to a particular risk, (b) different areas of professional expertise and views are appropriately considered in the management of risks and (c) sufficient information and evidence to facilitate risk oversight and decision making are provided.

4.2. Harm Table

Post Office assess each risk by demonstrating the relationship between the likelihood of the risk materialising (on a standard 1-5 scale) and the impact of the event should the risk materialise (again on a standard 1-5 scale) to provide an overall risk rating.

The Post Office corporate HARM table describes the impact/likelihood scales which must be applied. This is provided at section 9.2.

Each active risk should have 3 ratings namely:

- **Inherent**: the level of risk before any control activities are applied;
- **Current Residual**: the latest level of risk considering the effectiveness of the controls currently in place; and,
- **Target**: the level of risk that is desired when any planned additional controls have been implemented. This must be consistent with the associated approved risk appetite.

All of these should be recorded on the Post Office's Governance, Risk & Compliance tool.

4.3. Risk Hierarchy and Classification

Post Office has a three-level risk hierarchy. These are:

- **Enterprise Risks:** The Post Office's key business risks are grouped into fourteen enterprise-level themes which mirror HM Government's approach to enterprise risk classification (as described below). These risks are Post Office-wide and so are of corporate importance. Each enterprise risk is owned by a single GE member. Central Risk provide an update on the management of these enterprise risks at each RCC and ARC;
- **Intermediate Risks:** These are sub-categories of an enterprise risk to which they are linked. They are often the key risks faced by individual business areas; and,
- **Local Risks:** These are sub-categories of intermediate risks, to which they are linked. They are often more specific, local risks faced by individual business units.

The Post Office risks have been categorised as follows, consistent with those advocated by HM Government's 'Orange Book'[12]:

- **Strategy:** Risks associated with ineffective and poorly designed strategy, not aligned to the interest of its key stakeholder(s), unable to support the full integration of any acquired business, delivery of plans or objectives;

[12] HM Government: Management of Risk (Principles and Concepts) – June 2019

POL00423571

- **Governance:** Risks associated with ineffective and/or disproportionate oversight of decision making, unclear authorities and accountabilities across the management hierarchy, insufficient transparency on business performance;
- **Operational:** Risks associated with ineffective and inefficient internal processes, unsound and insufficiently assured control environment and ineffective continuity plans and recovery strategy;
- **Legal**: Risks associated a failure to comply with legislative and regulatory changes, act in accordance with legal and regulatory obligations (i.e. GDPR), sectoral regulator guidance and/or other external legal activity (i.e. litigation);
- **Health & Safety**: Risks associated with failure to provide a safe work environment for employees (including workplace and branches) and ensure physical safety of employees and agents in response to incidents such as theft, robbery, burglary, terrorism, pandemic and site safety (e.g. workplace COVID-secure);
- **Financial:** Risks associated with failure to provide adequate liquidity to meet financial obligations, having insufficient funding, uncontrolled costs, credit failure and increased taxation;
- **Commercial**: Risks associated with failure to implement unattractive commercial proposition due to high 3rd party dependency, capacity constraints, cost pressures, varied demand and skill shortages;
- **People**: Risks associated with ineffective leadership and engagement, sub-optimal culture, inappropriate recruitment model, insufficient capacity and capability, unattractive Postmasters proposition, industrial action and/or non-compliance with relevant employment legislation/HR policies;
- **Technology**: Risks associated with inadequate technology, inability to deliver the expected IT services and sustain competitive advantage in products/services;
- **Information**: Risks associated with failure to produce a robust, suitable, appropriate, correct and complete data/information and to exploit data/information to its full potential;
- **Security**: Risks associated with failure to prevent un-authorised and/or inappropriate access to the estate and information, including cyber security;
- **Change**: Risks associated with failure to implement change programmes and projects aligned with strategic priorities, consistent with budget allocation, deliver requirements and intended benefits to time, cost and quality;
- **Reputational**: Risks associated with adverse events including ethical violations and/or adverse stance to corporate social responsibility; and,
- **Marketplace & Brands**: Risks associated with failure to maintain a competitive advantage in response to actions adopted by main competitors, changes in customers service needs and expectations, loyalty to the Brand.

4.4. Risk Articulation

All risks across the risk hierarchy must be expressed in terms of their cause(s), the risk event itself, and their impact:

POL00423571

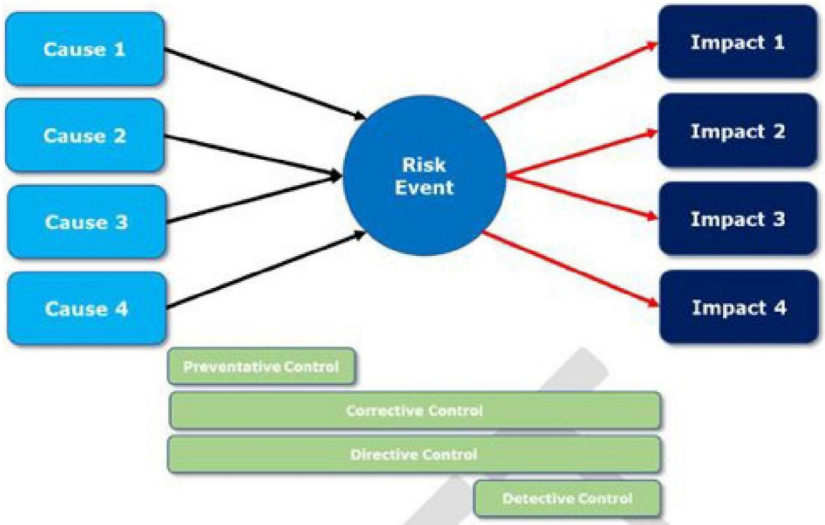


Figure 2: Post Office bowtie diagram

- **Cause**: A cause is an element which alone or in combination with other causes has the potential to give rise to the risk. They are generally (but not exclusively) external;
- **Event**: An event is an articulation of the potential adverse or beneficial circumstances that could result from the cause – in effect the risk itself. A risk may have multiple causes and consequences and can affect multiple objectives. Post Office risks should be classified (see section 4.3) against the Event not the Cause or the Impact; and,
- **Consequences/Impact**: Consequences are the outcome of a risk event materialising. Outcomes can be positive or negative. They can also be direct or indirect. It is also possible to express them qualitatively or quantitatively. They should be assessed using Post Office HARM table (see Appendix 9.2).

4.5. Governance, Risk & Compliance (GRC) tool

All Post Office risks (across all levels of the risks hierarchy) must be identified, analysed, evaluated and managed using the Central Risk GRC tool.

4.6. Incidents

All non-IT incidents should be reported by the Incident Reporter. The Incident Owner responds to incident based on the Post Office risk appetite, identifying the root cause as well as putting appropriate action plans and all controls in place.

By working closely with the respective Risk Business Partner, the Incident Owner must also consider any impact the incident has had on the current risks and controls (mapped where relevant) or whether the incident constitutes a new risk to the business that has not been recorded within the risk register. The Incident Owner manages action plans through to closure.

IT related incidents are reported (new) or escalated (existing) through the IT Service Desk.

POL00423571

5. Minimum Control Standards

Post Office has a number of minimum control standards which apply to the management of its risks.

They cover a range of control types (i.e. directive, detective, corrective and preventative) to ensure risks are managed to within the acceptable level of risk appetite.

Risk Policy Area	Risk Description	Minimum Control Standards	Accountability	Assessment Timing
Risk Governance (Roles & Responsibilities)	Risk that the GE and Post Office Groups do not perform their 1st line function and fail to proactively identify, assess, own and manage their risks and/or maintain their associated internal control measures	**Detective control**: Monthly, Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) review and update their risks (including current residual risk score, mitigating actions, target risk rating etc.) to the corporate GRC tool.	• Risk Leads • Risk Owners	Monthly
Risk Governance (Risk Reporting)	Risk that the GE is unable to fulfil its responsibility of having a sound understanding of risks facing Post Office	**Detective control:** Monthly, Central Risk Business Partner produce and circulate to their linked GE member a Risk Dashboard showing the latest position of their enterprise, key intermediate and local risks (including Risk Heatmap, risk weighting, risk trends etc) as reflected in the corporate GRC tool.	• Central Risk Business Partner	Monthly
	Risk that the Board, RCC/ARC are unable to fulfil their responsibilities of having a sound understanding of risks facing Post Office	**Detective control:** Bi-monthly, Central Risk produce and submit to RCC and ARC a Risk Dashboard showing the latest position of the group key enterprise, intermediate and change risks (including Risk Heatmap, risk weighting, risk trends etc.) as reflected in the corporate GRC tool.	• Central Risk	Bi-monthly
	Risk that Post Office Groups do not perform their 1st line function and fail to proactively monitor and update risk response to mitigate the risk	**Detective control:** Monthly, Individual Risk Owners (supported by their Risk Lead and Central Risk Business Partner) monitor that all risks have effective risk response outlining the actions appropriate to mitigate the risk and when a risk reaches its expected response date, review mitigation actions to either close the actions or postpone the due date, as reflected in the corporate GRC tool.	• Risk Leads • Risk Owners	Monthly
	Risk that the GE is unable to fulfil its responsibility of having a sound understanding of new and emerging risks facing Post Office	**Preventative control:** Bi-annually, Central Risk identify new and emerging risks likely to impact Post Office in the sectors in which competes and the environment in which operates. Summary of these risks is reported in the GE Risk trend paper submitted to GE members.	• Central Risk	Bi-annually

DRAFT

POL00423571

Risk Policy Area	Risk Description	Minimum Control Standards	Accountability	Assessment Timing
Risk Governance (Escalation Principles)	Risk that Post Office Groups fail to report and act appropriately to issues of concern	**Detective control:** Risk Owners escalate a risk to their relevant GE member or equivalent senior leader when they have insufficient authority to effectively manage the risk. The Risk Owner provide the receiving manager with complete information about the risk. Risk ownership can only be transferred when a risk has been escalated and accepted. Evidence of the acceptance is maintained by Central Risk Team in the corporate GRC tool.	• Risk Owners • Central Risk Business Partners	Ad-hoc
Risk Strategy (Risk Appetite & Key Risk Indicators)	Risk that Post Office Groups do not assess risk appetite in accordance with the Post Office Risk Appetite	**Preventative control:** Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) assess risk appetite against a 5-tiered scale, including open, flexible, neutral, cautious, averse risk appetite scale, as reflected in Post Office Risk Appetite Statement.	• Risk Owners • Risk Leads • Central Risk Business Partners	Ad-hoc
	Risk that the Risk Appetite statements and KRIs are not periodically reviewed and approved by Board/RCC/ARC	**Detective control:** Group Executive review Risk Appetite Statements and KRIs supported by the Central Risk as needed. Risk Appetite Statements and associated KRIs are approved by Board/ARC. Additional Risk Appetite Statements/KRIs are requested from Board/ARC to Group Executive, as necessary.	• Group Executive • Central Risk • Board/ARC	Ad-hoc
	Risk that the Risk Appetite statements and KRIs are not periodically monitored by Post Office Groups	**Detective control:** Group and individual Business Units monitor existing KRIs to determine adherence to Risk Appetite Statements that apply to the Group. Any concerns about the ongoing viability of existing Risk Appetite Statements approved by the GE /Board are raised by Group and individual Business Units. Areas of non-compliance to Group Executive and Board/ARC are escalated by Central Risk.	• Group and individual Business Units • Central Risk	Ad-hoc
Risk Strategy (Exceptions)	Risk that the business goes outside of existing procedures, legislation or regulation for new / existing process and do not consider how they can control and reduce the impact	**Preventative control:** A Risk Exception is requested using a Risk Exception Note (REN) where business requirements make it necessary to depart from an approved appetite or operate outside of existing procedures. The REN is completed by the Business unit/project manager and approved by the relevant GE member. All approved RENs are uploaded and monitored in the corporate GRC tool by Central Risk.	• Group and individual Business Units • Central Risk	Ad-hoc

DRAFT

POL00423571

Risk Policy Area	Risk Description	Minimum Control Standards	Accountability	Assessment Timing
Risk Strategy (Exceptions)	Risk that the Exceptions are not reviewed and updated regularly	**Detective control:** Monthly, Central Risk check if there are any overdue Risk Exception Notes and information requires updating as evidenced in the corporate GRC tool.	Central Risk	Monthly
	Risk that the GE is unable to fulfil its responsibility of having visibility on the open Post Office Risk Exceptions	**Detective control:** Bi-monthly, Central Risk report on all Risk Exception Notes to the GE and ARC, as reflected in the corporate GRC tool.	Central Risk	Bi-monthly
Risk Protocols (Risk Management Process)	Risk that Post Office Groups do not perform their 1st line function and fail to assess and evaluate their risks in line with the rating standards outlined in the Harm Table	**Preventative control:** Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) evaluate their risks in terms of their potential impact and likelihood in accordance to Post Office corporate Harm Table, as reflected in the corporate GRC tool.	• Risk Owners • Risk Leads • Central Risk Business Partner	Ad-hoc
	Risk that Risk Owners overstate the level of mitigation against specific risks, thereby understating the risk likelihood / impact	**Detective control:** Internal Audit through their annual audit programme will assess the effectiveness of controls and report controls that are not designed or operating effectively to mitigate the state risk.	Internal Audit	Ongoing
Risk Protocols (Harm Table)	Risk that Post Office HARM table does not reflect the current corporate view on the calibration of impact and likelihood risk ratings	**Preventative control:** Annually, Post Office Harm Table is reviewed by GE members with the support of the Central Risk. Reviewed Harm Table is submitted for approval by Central Risk to ARC.	• GE • Central Risk • ARC	Annually
	Risk that Post Office Groups do not perform their 1st line function and fail to properly score their risks	**Preventative control:** Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) score their risks against the inherent, current residual and target risk rating as reflected in the corporate GRC tool.	• Risk Owners • Risk Leads • Central Risk Business Partner	Ad-hoc
Risk Protocols (Risk Articulation)	Risk that Post Office Groups do not perform their 1st line function and fail to properly articulate their risks	**Preventative control:** Individual Post Office Risk Owners (supported by their Risk Lead and Central Risk Business Partner) articulate their risks in terms of their cause(s), the risk event itself, their impact and classified against the event, as reflected in the corporate GRC tool.	• Risk Owners • Risk Leads • Central Risk Business Partner	Ad-hoc

DRAFT

POL00423571

6. Linked material & Contacts

6.1. Linked material

This Policy is underpinned by the Risk Management Framework and other supporting risk material accessible on Post Office Central Risk intranet site.

This Policy is consistent with, and aligned to, other Post Office policies and standards including, but not limited, to:

- Anti-Bribery & Corruption Policy
- Business Continuity Management Policy
- Change Policy
- Code of Business Standards
- Financial Crime Policy
- Health and Safety Policy
- IT Disaster Recovery
- Risk Management Framework
- Treasury Policy
- Vulnerable Customer Policy
- Whistleblowing
- Internal Audit Charter

6.2. Contacts

Post Office Head of Risk or Central Risk team.

DRAFT

POL00423571

7. Governance

Post Office Chief Finance Officer is the Policy sponsor.

Post Office Head of Risk is Policy owner. They are accountable for ensuring that the Central Risk team provides assurance over compliance with the Policy and the supporting the Risk Management Framework.

The Policy will be reviewed every year. ARC will approve any changes.

DRAFT

POL00423571

8. Definitions

Appetite
This is the level of risk that the Group is prepared to accept or pursue or before action is deemed necessary to reduce it; also, sometimes called 'risk tolerance'.

Control
This is any action taken to reduce the likelihood and/or magnitude of a risk.

Exception
There are on occasion exceptional situations where business requirements make it necessary to depart from an approved policy and operate outside of risk appetite. In these circumstances the business can choose to accept this risk and formally request a risk exception for a defined period of time.

Governance
This is the system by which organisations are directed and controlled. It defines accountabilities, relationships and responsibilities in the organisation as well as determine the rules and procedures and monitors performance.

Impact
This is the estimated result including financial, operational and reputational that would be realised if a risk event would occur.

Incident
An incident is an event, where individual operational controls either did not exist or did not operate as intended, or the incident was not anticipated, and which has, or could have, resulted in a financial impact (direct or indirect), a regulatory implication, a customer consequence or a significant operational impact.

Likelihood
This is the evaluation or judgement regarding the chances of the risk materialising. Likelihood is also called 'probability' or 'frequency'.

Risk
Risk is defined as the effect of uncertainty on the Post Office achieving its strategic objectives. That effect may be positive, negative or a deviation from the expected. Risks are described in terms of causes, potential events and their consequences.

Risk Management
This is the co-ordinated activities designed and operated to manage risk and exercise internal control within an organisation.

DRAFT

POL00423571

9. Appendices

9.1. Risk Appetite scale

	Appetite rating	Risk taking philosophy	Tolerance for Uncertainty[13]	Decision choice[14]	Prioritisation of Strategic Objective[15]
	Open	Will take risks and **accept the possibility of failure**	Will **accept the possibility of failure**	Will choose the **option with the highest return**	**Will accept risks could materialise** and the achievement of (some) strategic objectives could be compromised
	Flexible	Will **take justified risks**	Will choose the option which has **some degree of risk**	Will accept risks materialising subject to being **able to proactively manage their adverse impact**	**Will accept (under certain conditions) risks could materialise** the achievement of (some) strategic objectives could be compromised
	Neutral	**Prefers, on balance, safe delivery to risk taking**	Will **accept, on balance, risks** could materialise	Will accept risks could materialise but only if **adverse impact is limited and heavily outweighed by benefits**	Would **prefer ideally not to accept** risks materialising if this meant the achievement of (some) strategic objectives could be compromised
	Cautious	Will take a **conservative approach to risks**	Will **accept some risks** could materialise	Will accept some risks materialising but only if activity is essential and the **possibility and extent of failure is limited**	Would be **somewhat reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised
	Averse	Will **avoid nearly all risks** where at all possible	Has an **extremely low appetite for any risks** to materialise	Will always select the option with the **lowest risk**	Would be **extremely reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised

[13] **Tolerance for uncertainty**: How willing is Post Office to accept uncertain outcomes? This illustrates the Board's appetite to trade off certainty to achieve a given objective. A low rating demonstrates the Board's need for certain outcomes, while a high rating shows the Board will pursue an objective even with an uncertain outcome.

[14] **Decision choice**: When faced with multiple decision options, how is Post Office willing to select a decision that puts a strategic objective at risk? This question assesses the Board's acceptance that a given choice may lead to failure to meet a strategic objective. A Board who are averse will only choose options that pose a minimal threat to the strategic objective's achievement. A Board open to this risk are willing to trade off the possibility of failure for a high-risk, high-reward decision.

[15] **Prioritisation of strategic objective**: How willing is Post Office willing to trade off this specific objective against achievement of other objectives? This demonstrates the Board's willingness to pursue achievement of a given strategic objective over achievement of another. A Board who are averse to this would never trade off completing the objective in question for failure of other objectives. A Board which is open would be willing to accept this trade-off.

POL00423571

9.2. HARM Table

RISK SCORING	IMPACT ON								
	Financial (inc. strategic)	Operational (inc. people, change technology, information security)	Customer	Reputational (inc. third party, legal and regularity)					
Critical - 5	£20m> or could have a long term impact on commercial viability	– Exceeds operational capacity to respond, breach of Government commitments – Fatality and/or prosecution – Loss of critical system or complete network outage	– Significant boycott of products and services – Breach of coverage or scope of services to meet social purpose or entrustment	– High profile legal case – Maximum regulatory penalties, removal of ability to operate, public enquiry – Complete loss of confidence e.g. staff, clients, partners, customers – Sustained hostile national media coverage and online narrative	A(5)	A(10)	A(15)	A(20)	A(25)
Major - 4	£5m> - <£20m or could substantially weaken the business	– Major operational impact felt throughout the business – Multiple major injuries – Partial loss of critical systems or critical system vulnerabilities left unpatched	– Alienate/lose a significant group of customers, Postmasters or partners	– Material legal dispute with negative outcome – Substantial censure sanctions imposed or large scale penalties, material customer detriment – Minister exercising powers, parliamentary inquiry – Major adverse national media campaign	N(4)	N(8)	A(12)	A(16)	A(20)
Significant - 3	£100k> - <£5m or significant effect on achieving business objectives	– Operational impact felt in multiple areas – Major injury with adverse HSE outcome or multiple minor injuries e.g. assault on branch – Significant loss of systems	– Customer / Postmaster dissatisfaction impacting business achieving objectives e.g. innovation – Safeguards and controls to protect vulnerable customers	– Reportable to regulators, m sanctions, small fines, minor/no customer detriment – Minister discussion – Substantial adverse national media campaign	T(3)	N(6)	N(9)	A (12)	A (15)
Moderate - 2	£50k > - <£100k or moderate effect on achieving business objectives	– Small operational impact felt to a single area – Minor injury with adverse HSE outcome or major injury with no personal liability outcome – Moderate loss of non critical systems	– Small number of customers contained within 1 product or channel, or where there is no scope for customer, Postmaster or partner detriment	– Low level repeated penalty breaches e.g. waste water – Adverse notification from regulators – Some adverse media and online reaction	T(2)	T (4)	N(6)	N(8)	N(10)
Minor - 1	£0> - <£50k or negligible effect on achieving business objectives	– No measurable operational impact to business – Minor personal injury with accidental outcome – Insignificant loss of systems	– No or very minor customer impact to a small number of customers, Postmasters or partners	– Low level legal issue – No regulatory impact e.g. penalty notice – Little media / online reaction	T (1)	T(2)	T(3)	T(4)	N(5)
					Remote - 1	Unlikely - 2	Possible - 3	Likely - 4	Almost Certain - 5
					Almost an inconceivable event	Event is unlikely but could occur	Event is still unlikely but more possible to happen	Risk will probably occur in most circumstances	Risk is expected to occur in most circumstances or has materialised
					LIKELIHOOD				

DRAFT

POL00423571

10. Control

10.1. Policy Version

Date	Version	Updated by	Change Details
1 November 2019	1.0	Jenny Ellwood	Reviewed and refreshed to reflect new Head of Risk position and ensure Business hold accountabilities for identification and management of their risks
1 November 2020	1.1	Mark Baldock	Annual review and amends

10.2. Policy Approval

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

Committee	Date Approved
POL RCC	
POL ARC	

Policy Sponsor: Chief Finance Officer
Policy Owner: Head of Risk
Policy Author: Central Risk Team
Next review: November 2021

10.3. Company Details

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

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

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

DRAFT

POL00423571

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

3.1

Title:	Risk Appetite & Key Risk Indicators: A Proposed Approach	**Meeting Date:**	12 November 2020
Author:	Mark Baldock, Head of Risk	**Sponsor:**	Al Cameron, Group Chief Finance Officer

Input Sought: Noting & Approval

The Risk & Compliance Committee (RCC) is asked to approve that the approach to Risk Appetite and Key Risk Indicators (KRIs), which will:

- be primarily articulated at the enterprise risk level;
- be assessed against a 5-tiered scale;
- be tailored for different enterprise risks;
- take into account our willingness and capacity for taking risks and our level of maturity in managing them;
- be managed using the 3 lines of defence model;
- be reported monthly as part of the Group Executive (GE) Dashboards and every two months as part of the RCC/ARC Dashboards; and
- be subject to yearly review;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

The Committee is also asked to note that, subject to approval, the approach will be initially applied to 3 enterprise risk groupings namely (i) **Legal & Compliance**, (ii) **Operational** and (iii) **Technology & Security**. Their specific application will be subject to separate approval by the RCC and the ARC, currently targeted for January 2021.

Executive Summary

This paper seeks RCC approval to the Post Office's approach to Risk Appetite and Key Risk Indicators (KRIs). It describes:

- the principles that underpin the approach
- the associated benefits
- how Risk Appetite and KRIs should be assessed
- how accountability should work
- proposed Next Steps and the indicative timeline

The Post Office's approach is based on industry best practice.

Confidential

POL00423571

Report

- What are Risk Appetites and Key Risk Indicators and why are they important?
- What are the principles that underpin our proposed approach?
- How have we approached this work?
- What are the proposed Next Steps and the indicative timeline?

Background

1. The Post Office's draft Risk Policy[1] is organised around 3 themes namely (i) **Risk Governance** (which focuses on how Post Office risk management activity is organised), (ii) **Risk Strategy** (which considers the Post Office's overall approach to risk management and (iii) **Risk Protocols** (which defines the risk management activities that must be undertaken.

2. The Risk Strategy component is specifically concerned with the techniques by which Post Office should assess risks. This includes **an approach to Risk Appetite** and **Key Risk Indicators (KRIs)** such that we can meet our strategic objectives of (i) supporting Post Office Postmasters, (ii) building a fit for purpose network and, (iii) focusing relentlessly on Post Office core strengths and customers.

3. This paper details the Post Office's specific approach to Risk Appetite and KRIs. These are defined as follows:
   - **Risk Appetite**: The amount of overall risk an organisation is willing to pursue (or retain) to achieve its strategic objectives. It is a qualitative assessment generally made at enterprise risk level.
   - **KRIs**: The measures put in place to show the underlying trend of specific risks. KRIs are predictive. They are a set of 'guide rails' to provide context within which individual risk impact and likelihood ratings can be considered. KRIs are a quantitative assessment again generally made at enterprise risk level.

Approach

4. Our approach is based on industry-standard principles[2] namely:
   - Scope: Our Risk appetite/KRIs will be primarily articulated at the enterprise risk level but will also help guide/shape the management of linked (but subsidiary) intermediate and local risks;
   - Complex: Our Risk appetites/KRIs are likely to be complex. Excessive simplicity, while superficially attractive, may be counter-productive;
   - Measurable: Our Risk appetites/KRIs will be measurable so will be based on relevant, accurate and readily available existing data;
   - Flexible: They will not be single, fixed concepts. There will be different (and tailored) appetites for different enterprise risks; and,
   - Manageable: Our approach will take account our risk management capability, our willingness and capacity for taking risks and our level of maturity in managing them.

[1] The Post Office's draft Risk Policy v1.1 has been tabled separately for RCC/ARC approval in 11/2020.
[2] Institute of Risk Management: Risk Appetite & Tolerance Guidance paper – 9/2011. Gartner: Ignition Guide to Drafting and Operationalizing Risk Appetite – 2/2020

Confidential

POL00423571

Benefits

5. We consider such an approach will:
   - allow the Board, GE, RCC and ARC to understand our aggregated levels of risk to determine acceptability or not;
   - provide assurance that our strategic objectives will be secured and provide early warning where achievement is under threat;
   - allow the business to focus limited resource to manage risks outside of tolerance and tolerate risks which lie within the thresholds;
   - support GE in understanding the degree to which the business is exposed to the consequences of a risk event; and,
   - be able to flex and adapt to the changing business environment.

Assessment

6. We propose the Post Office assess appetite (at the enterprise level) against a 5-tiered scale which ranges from '**Averse**', through '**Neutral**' to '**Open**.'

7. We will also take into account other factors including our **tolerance for uncertainty** (how willing are we to trade off certainty to achieve an objective), **decision choice** (how willing are we to make a decision, from a number, that risks a strategic objective) and **strategic priority** (how willing are we to trade off an objective against achievement of other objectives)

8. Our proposed Risk Appetite scale is provided at Appendix 1.

Accountability

9. The Post Office's '3 lines of defence' risk management governance structure will oversee both the initial application, and ongoing management, of our approved Risk Appetites and KRIs as follows:

1st Line	Board/ARC[3]	• Approve all final draft Risk Appetite Statements and associated KRIs. • Request, as necessary, the Group Executive commission work to articulate additional Risk Appetite Statements/KRIs • Seek assurance Post Office is adhering to approved Risk Appetite Statements/KRI thresholds
	Group Executive	• Effectively and clearly communicate goals and objectives, strategy, achievement metrics, and relevant time periods for pursuing the objectives related to developing risk appetite statements. • Set the Risk Appetites and approved tolerance levels that ensure enough risk is being taken to ensure Post Office strategic objectives are met • Secure Group Command consensus on statements and approach. • Commission revisions of Risk Appetite Statements and KRIs as needed.
	Group and individual Business Units	• Validate or raise concerns about the ongoing viability of existing Risk Appetite Statements approved by the GE /Board • Monitor existing KRIs to determine adherence to Risk Appetite Statements that apply to the Group
2nd Line	Central Risk	• Produce Post Office corporate policy/standards for Risk Appetite and KRIs • Develop (in discussion with 1st Line) initial set of corporate Risk Appetite Statements and KRIs • Facilitate ongoing development of new (and enhancements to existing) Risk Appetite Statements and KRIs • Provide assurance of 1st Line compliance with standards in this area • Escalate areas of non-compliance to Group Executive and Board/ARC

[3] After initial RCC discussion and approval

Confidential

POL00423571

3rd Line	Internal Audit	• Provide, as part of its agreed Audit plan, an independent and objective evaluation of the adequacy and effectiveness of the risk management and control, making recommendations for improvement • Report to RCC/ARC on its findings, particularly around areas of non-compliance

Reporting

10. Following RCC/ARC approval of the individual Risk Appetites (and linked KRIs) for specific enterprise risk groupings the target risk ratings of the relevant enterprise risk as well as each linked (but subsidiary) intermediate and local risks will be calibrated to ensure alignment.

11. This will mean that any risk in this grouping
    - identified as being **outside of appetite** must be proactively **treated** with mitigation actions clearly articulated, owners allocated, and dates identified;
    - assessed as being **within appetite** can be simply **tolerated** such that no further mitigations will be required.

12. Central Risk will include an assessment of enterprise risks against their approved Risk Appetite (along with the latest KRI trends) as part of the monthly GE Dashboards and bi-monthly RCC/ARC Dashboards

13. An illustrative Dashboard is provided at Appendix 2.

Next Steps

14. The RCC are asked to **approve** that our Risk Appetites and KRIs and **note** that, subject to approval, the approach will be initially applied to 3 enterprise risk groupings namely (i) **Legal & Compliance,** (ii) **Operational** and (iii) **Technology & Security**. This will be subject to separate RCC/ARC approval, currently targeted for 1/2021.

Appendix 1: Post Office Risk Appetite scale
Appendix 2: Post Office Risk Appetite Tracker & KRI's

Confidential

POL00423571

Appendix 1: Post Office Risk Appetite scale

	Appetite rating	Risk taking philosophy	Tolerance for Uncertainty[4]	Decision choice[5]	Prioritisation of Strategic Objective[6]
	Open	Will take risks and **accept the possibility of failure**	Will **accept the possibility of failure**	Will choose the **option with the highest return**	**Will accept risks could materialise** and the achievement of (some) strategic objectives could be compromised
	Flexible	Will **take justified risks**	Will choose the option which has **some degree of risk**	Will accept risks materialising subject to being **able to proactively manage their adverse impact**	**Will accept (under certain conditions) risks could materialise** the achievement of (some) strategic objectives could be compromised
	Neutral	**Prefers, on balance, safe delivery to risk taking**	Will **accept, on balance, risks** could materialise	Will accept risks could materialise but only if **adverse impact is limited and heavily outweighed by benefits**	Would **prefer ideally not to accept** risks materialising if this meant the achievement of (some) strategic objectives could be compromised
	Cautious	Will take a **conservative approach to risks**	Will **accept some risks** could materialise	Will accept some risks materialising but only if activity is essential and the **possibility and extent of failure is limited**	Would be **somewhat reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised
	Averse	Will **avoid nearly all risks** where at all possible	Has an **extremely low appetite for any risks** to materialise	Will always select the option with the **lowest risk**	Would be **extremely reluctant** to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised

[4] **Tolerance for uncertainty**: How willing is Post Office to accept uncertain outcomes? This illustrates the Board's appetite to trade off certainty to achieve a given objective. A low rating demonstrates the Board's need for certain outcomes, while a high rating shows the Board will pursue an objective even with an uncertain outcome.

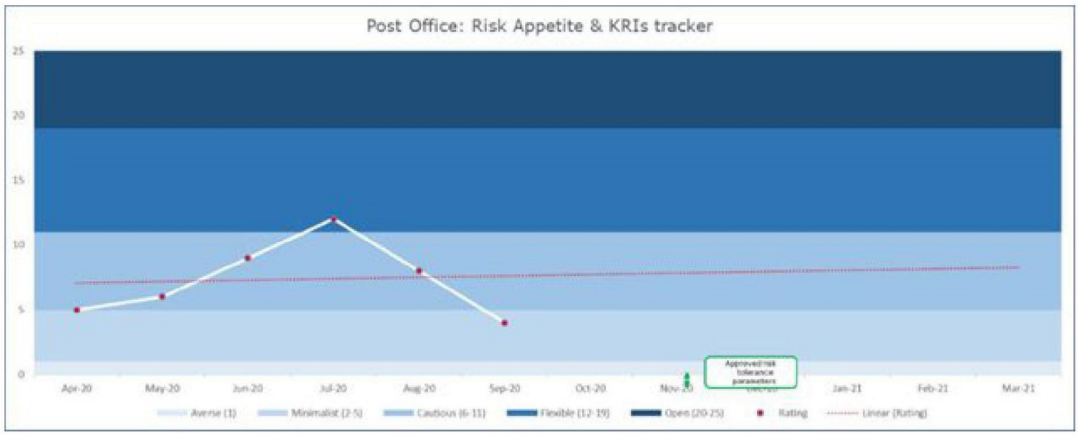
[5] **Decision choice**: When faced with multiple decision options, how is Post Office willing to select a decision that puts a strategic objective at risk? This question assesses the Board's acceptance that a given choice may lead to failure to meet a strategic objective. A Board who are averse will only choose options that pose a minimal threat to the strategic objective's achievement. A Board open to this risk are willing to trade off the possibility of failure for a high-risk, high-reward decision.

[6] **Prioritisation of strategic objective**: How willing is Post Office willing to trade off this specific objective against achievement of other objectives? This demonstrates the Board's willingness to pursue achievement of a given strategic objective over achievement of another. A Board who are averse to this would never trade off completing the objective in question for failure of other objectives. A Board which is open would be willing to accept this trade-off.

Confidential

POL00423571

Appendix 2: Risk Appetite/KRI tracker (illustration)



	Apr-20	May-20	Jun-20	Jul-20	Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Jan-21	Feb-21	Mar-21
KRI 1												
KRI 2												
KRI 3												
KRI 4												

Illustrative Commentary

The approved risk appetite for this specific enterprise risk grouping is **Averse**. This means the Post Office will avoid taking pretty much any risk in this area where at all possible and has an extremely low appetite for any such risk materialising.

The current enterprise risk is currently assessed at 2:2 in terms of its potential adverse impact and the likelihood of it materialising. Although year to date trends show the risk rating has been reducing in recent months it remains **outside of appetite**. As such further mitigations are required in addition to those already in place to reduce the risk further.

Although 3 of the 4 KRIs are trending Green there is some evidence of volatility in recent months which, if it continues, will place increasing pressure on the enterprise risk rating even if, in the near future, it is brought within tolerance.

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.2

Title:	Compliance and Audit Report	**Meeting Date:**	12 November 2020
Author:	Jonathan Hill: Director, Compliance Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer Ben Foat: General Counsel

Input Sought: Noting

The Committee is asked to:

1. note the Compliance update, in particular:
   - The Telecoms incident in respect of customer communications, which has been reported to Ofcom;
   - The branch registration errors with HMRC for Travel Money;
   - The financial crime risk of Capita's (a Post Office bill payment reseller) MSB customers and the need to review all bill payment reseller controls;
   - The temporary suspension of conduct risk branch mystery shopping during the latest Covid-19 national lockdown

and;

2. note the Internal Audit update, specifically progress being made with delivery of the Internal Audit programme and completion of audit actions;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position.

Confidential

POL00423571

Compliance

Telecoms

Comms incident

1. On 17 September 2020, Fujitsu notified Post Office of a P1 incident affecting inbound and outbound customer communications between February and September. The total number of affected inbound comms is 7,846 and the number of affected outbound comms is 153,684 (following a deduplication process as some comms are issued in two formats). The outbound comms has impacted c.107,300 unique customers.
2. Some of the communications are regulated and could result in consumer harm. The Post Office breach protocol process was followed and Meredith Sharples informed Ofcom verbally on 27 September of the incident. This was followed up with a detailed letter on 23 October. Ofcom are now reviewing the content of the letter and deciding on whether to open a formal investigation. A copy of this letter is attached in Appendix 1.
3. Given the variety of outbound communications that have been impacted, addressing and rectifying consumer harm has been a complex process as there are 33 different comms that were impacted which include, but not limited to, cease notifications, overdue payment reminders, confirmation of engineer appoints. The team have prioritised their work according to the impact on customers as set out in the table below. Details of the specific comms impacted was provided to Ofcom.

Priority	**No. of impacted comms (not customers)**
1. Customer's services were ceased	2,877
2. Potential financial impact on the customer	115,830*
3. Customer inconvenienced - communications relates to regulation	3,650
4. Customer inconvenienced - communications does not relate to regulation	21,133
5. No customer impact	9,551

* Please note that 99,689 of the priority 2 comms are e-bill notification communications where we inform the customer that their bill is ready online.

4. The final RCA with Fujitsu is still being worked through. However, we understand that the main cause of the incident is a result of a file that become too large. Once deleted this appears to have rectified the issue. Fujitsu have put in further checks to confirm that outbound comms are going out and inbound comms are arriving correctly.
5. Of the 7,846 inbound communications, the Fujitsu team has reviewed 2,644 as at 5th November. Where any consumer harm is identified the customers are being made good, as if the communications failure had not happened. The Post Office team is checking the remediation work being done by Fujitsu. We are pressuring Fujitsu to confirm when it expects to have completed this exercise and are pushing for it to be closed by end November/early December.

Fairness

6. Post Office met Ofcom on 20th October to discuss how Post Office is meeting the Fairness Commitments we have signed up to. Ofcom view these commitments as "reputational regulation" whereby they publicly expose Communication Providers for practices that they believe are unfair. Ofcom expressed appreciation for the work done but continued to

POL00423571

reference Post Office having a high pricing differential between in contract and out of contract customers. This was explained by the telecoms team as being a result of having low acquisition pricing, thus driving a larger gap. This is not abnormal for the industry. Ofcom made no further comment and, as a result, no action is being be taken by the Telecoms Team other than to monitor the differential. If this became greater we could expect Ofcom to ask more questions, although we think it is more likely that it will address this at an industry level.

7. Ofcom plan to issue a statement with press coverage on their review of the market early next year to "name and shame" the worst providers as well as note good practice. We are expecting further informal follow up questions. Ofcom were understanding that our current position in the sale process meant that we were limited in our ability to make changes currently. This means that no action needs to be taken right now. However, once the sale process/RFP status becomes clearer this will need to be reassessed.

Annual Best Tariff Notifications

8. The telecoms team have delayed the implementation of the introduction of Annual Best Tariff Notifications from October to December2020, within the regulatory timetable. These letters will inform customers who are currently out of contract that they could save money by signing up to a new contract and will present Post Office's best offers. The ABT must be sent by 14th February 2021 and there is a very low risk to the implementation deadline however the letters are expected to drive more calls to the contact centre and drive complaints as people will query why their current price is higher than the new offers in their communications.
9. Ofcom had previously expressed concerns about the amount Post Office customers who are out of contract. According to Ofcom the average number of out of contract customers in the industry is 40%, (the highest is 61% and lowest is 24%)[1]. Post Office have 58% customers who are out of contract, however some of these customers are on rolling 30 day contracts and would not necessarily be better off moving to a longer-term contract. If these customers were not included, it is estimated that Post Office would be below 50%. As noted below, we are due to start sending Annual Best Tariff Reminders to customers, which we expect will further alter the percentage. Of the customers receiving the ABT notifications, the Telecoms Team anticipate 5% will churn and 35% of customers will re-contract onto new pricing. The Team will evaluate the effectiveness of the reminders before reviewing any further action.

Voice only customers

10. Post Office met with Ofcom on 1st October to discuss their plans for the voice only market. In 2017, Ofcom reached a voluntary agreement with BT to reduce its pricing for voice only customers by £5. This voluntary agreement is set to end at the beginning of next year and Ofcom confirmed during the meeting that they are looking to agree a further voluntary agreement with BT. We are now awaiting the consultation which will detail the agreement so that we can assess the impact to Post Office. We expect the impact to be minimal as Ofcom thought the introduction of retail price regulation would be unlikely and are looking to have a similar basket control that was agreed before.

European Electronic Communications Code

11. Ofcom have now issued their statement and consultation on the European Electronic Communications Code and detailed the regulations they plan to introduce. This requires significant changes to be made in telecoms however Ofcom have staggered the implementation deadlines, with the first tranche not due to be implemented until

[1] https://www.ofcom.org.uk/__data/assets/pdf_file/0031/199075/bb-pricing-update-july-20.pdf



December 2021.

12. Please refer to Appendix 2 for a summary timeline of all key regulatory developments. This has been noted in the Law and Trends Forum.

Data Protection

GLO and Historic Shortfall Scheme

13. Compliance continues to work with the Historical Matters Unit to identify, locate and provide all data required to support the various ongoing initiatives, in particular:
    a. Servicing 220 Data Subject Access requests that vary in complexity from access to Shortfall information through to full requests requiring extensive searches of Post Office systems and archives.
    b. Considering the implications of information to be provided to the Enquiry which includes personal data relating to the 2015 Mediation Scheme. We continue to work with internal Legal on making a representation to the Enquiry to provide pseudo-anonymised data rather than full disclosure.
14. Post Office continues to receive a higher-than-normal number of complex FOI requests in relation to Historic Matters.
15. Given the sensitivity of these requests, Post Office is working with external Counsel, Legal and Communications on the responses and, where appropriate, decisions on disclosure are referred to the HMU Steerco. We continue to meet the FOI response timelines as set out in legislation and we have had no complaints from the ICO in respect of our handling of these cases.
16. Examples of FOI requests since the September RCC include:
    a. The number and value of Transaction Corrections issued by Post Office over the last 12 months
        i. The business does not hold the information in the format that was requested by the individual. by the individual.
        ii. FOI does not require an organisation to create new information, neither is it advisable to do so. to create new information, neither is it advisable to do so.
        iii. However, recognising that the information requested would be useful for resolving HSS claims the Data Protection, HSS and business teams have worked up a process that will allow for accurate Transaction Correction information to be issued to HSS applicants and to the HSS resolution team to verify claims. accurate Transaction Correction information to be issued to HSS applicants and to the HSS resolution team to verify claims.
    b. Information relating to 'out of date' scratch cards and whether Postmasters suffered any losses as a result of this.
        i. Where scratch cards went out of date Post Office should have carried the loss and not passed it through to Postmasters. However, anecdotally it is reported that some Post Office auditors who had identified out of date scratch cards in branches recorded this as a loss against the Postmaster.
        ii. Despite extensive searches across the business, we cannot definitively say whether Postmasters suffered a loss or not.
        iii. KPMG is working with HMU on the Post Office response to the judgements and this is one area that it will be examining to give a definitive answer.
        iv. We expect that the FOI request will be re-issued by the requester where, given the KPMG work, Post Office should be better placed to respond.

AWS Move to the Cloud:

17. Good progress is being made from a Data Protection perspective. Questionnaires continue to be received from upstream clients and are managed on a case-by-case basis. There are no significant concerns regarding the move to the Cloud and confidence remains high of

POL00423571

Client acceptance of the move.

18. The DP team are currently working with the Project to map out the Privacy Impact Assessments that will need to be completed and remediated against prior to going live. At this stage we are not anticipating any significant risks that will hinder progress.

GDPR Contract Remediation

19. The Contract Remediation project was formally closed at the end of July as reported to the previous RCC. Work is ongoing on and the number of outstanding contracts has reduced from eight to seven since the last RCC
20. Of those seven, four are awaiting execution and will be completed by the end of November.
21. Negotiations on the three remaining contracts (Fujitsu, Santander and Kinto (formerly Inchcape)) are close to completion with no significant barriers to execution.
22. Monthly CRG meetings continue to monitor progress and support negotiations. This will continue until all outstanding contracts are finalised.

Financial Crime

Compliance with Money Laundering Regulations

23. Following the permanent removal of 3,257 and pausing of 2,679 HMRC branch registrations in May 2020, it has been identified that 6 of the branches that were de-registered as part of this exercise have completed Travel Money transactions (25 transactions totalling £6,784.30 between 1st June (HMRC annual registration date) and 28th October 2020). Post Office is in breach of the regulations in respect of these branches.
24. The IT/Data team have identified historic inconsistencies between Post Office MDM data and Fujitsu RMD data records, which has caused the issue – a further 35 branch records are inaccurate, but this has not resulted in transactions to date. A root cause analysis and correction are still under investigation at the time of writing. We will investigate where the failure occurred and report back on the appropriate remediation steps to ensure that branches cannot transact when they are de-registered and/or what assurance can be provided to reconcile the data between Post Office and Fujitsu.
25. We verbally self-reported the issue to HMRC on 3rd November 2020 and have arranged for the premises to be registered. All of the relevant agent data is held from previous declarations and can be supplied on the November monthly HMRC report. Given the previous fine of £800k for premises registration issues in 2016, HMRC may decide to levy a financial penalty. However, on the basis that there are only 6 impacted branches for a 5 month period, and limited transactions, we may avoid penalty (previously c.900 premises were involved going back a number of years). A full written report will be sent to HMRC by 6th November 2020 once IT/Data investigations have progressed.
26. Suspicious Activity Reports (SARs) and investigations continue to rise, with 1,427 SARs and 157 investigations in August & September (up from 566 and 111 in August & September 2019). This is driven by branches raising concerns with large and multiple cash deposits, particularly relating to money transmission businesses. There is also evidence of changing criminal behaviour due to Covid and the economic uncertainty which is likely to further drive up suspicious activity in our Network and result in more SARs. We are working closely with Network teams to ensure customer-facing staff are made aware of the risks and their responsibilities.
27. We continue to work with banks through the National Economic Crime Centre Project Admiralty and the Banking Framework members to address the risks of cash laundering via Post Office. We continue to discuss particular activity with 2 banks in relation to significant cash deposits at Whitechapel and Philpot Street in East London where we continue to see

POL00423571

£5-7m per week deposited. These banks are currently analysing these deposits, and we have been advised that some relationships are being exited by them, but we expect a full response from them in November. If the banks are unable to provide assurances that the cash deposited is in line with their KYC, we will ask the banks to make alternative arrangements for these deposits.

28. From 20th August to 26th October, 23 Banking Framework cases were investigated (up 35% on the 2019). A number were complex cash deposit cases involving multiple accounts and banks. To help with increased workloads, a fixed term contract PO started mid-October, funded to the end of 2020/21. We continue to monitor volumes and their drivers but suspect this will need to be a permanent resource in 2021/22.
29. From intelligence provided by us, recent law enforcement activity concerning cash deposits in South and East London resulted in an individual arrested and money seized at one branch in connection with money laundering offences, we are aware of ongoing investigations.
30. A meeting was held with our new HMRC regulatory supervisor on 30th September. HMRC have indicated that they will not be undertaking proactive supervision activity or branch visits whilst Covid issued continue.
31. A response was submitted to HMT in respect of the Economic Crime Levy Consultation. The paper indicated that their preferred option is to have a revenue based levy with some exemptions for small businesses where it is not cost effective to gather the levy. We have put forward a position that as all POL regulatory revenue is derived via payment of dividend and commission from FRES, who are also regulated and subject to the levy, this would effectively be a 'double-levy' and therefore POL revenue should be exempt. We are unlikely to see a response to the consultation, and the draft legislation until the new year.
32. The risk assessment process was presented at the Commercial lead team meeting and have since seen an improvement in stakeholder engagement.

Anti-Bribery and Corruption ("ABC") update

33. Annual ABC training has been completed in September – overall completion is at 96.5% as at 2nd November 2020, however one Business Unit is at 81.7%, and this unit is being chased.

Whistleblowing Update

34. There has been an increase in new reports during August & September 2020 - 8 compared to 5 in the same period last year. The majority have been received from agent assistants and relate to allegations concerning Postmaster activity. There are no trends or issues, and all investigations are proceeding.
35. We are procuring some initial consultancy work with Protect (UK Whistleblowing Charity) to benchmark our whistleblowing policy and processes and help us to identify if there are any control gaps. We are also working with the Postmaster Complaints project to ensure that there is a centralised view of postmaster complaints or reported concerns. We have provided copies of our policy and procedures to the HMU Public Inquiry team.

Fit & Proper update

36. There have been a number of teething issues with the new agent F&P system and processes. A number of technical fixes have been delivered but some issues remain open and subject to further investigation:
    - Errors in Power BI reports produced to drive branch revocation and HMRC reporting
    - Data refresh issues

POL00423571

- People data extraction from the Financial Assessment is more cumbersome and labour intensive than first thought due to missing data on the report
- Legal Status discrepancies are being identified which were not corrected in previous declarations. They are being managed but are taking time and resource in F&P Ops, the Contracts and onboarding teams.
- Development of F&P Release 2 to bring in scope MoneyGram only branches and 'paused' bureau branches is on track with a view to deploying into production before the November change freeze, but this will require changes to processes and bedding in of new reporting.
- Self-serve declarations for Sole Traders via Branch Hub is also being developed by Accenture with the intention to have in place for January 2021.

37. These issues are being managed and overseen by the F&P Ops team manager who has built up expertise since taking on operational responsibility earlier this year, but his role is at risk in the new structure and the work is being transferred to another area. The F&P project has been closed, therefore the project team has now been disbanded and no longer able to provide any oversight or support. If the current F&P Ops manager leaves the business, and the work is transferred to a new manager, there is a risk that the current issues will take longer to resolve and regulatory obligations may not be met. We are liaising with HR to ensure that an appropriate owner is found and a remediation plan for the aforementioned issues is finalised. This will be brought back to the next RCC/ARC.
38. There are a significant number of changes to roles and responsibilities caused by OE. Due to the consultations, information on the changes is not available, and therefore keeping employee F&P tests up to date is challenging. We are working with HR to identify people leaving the business or moving into impacted roles.

External Threats

39. We have identified a growing trend of suspicious high volume Amazon voucher purchases, relating to potentially vulnerable customers who fall victim to fraudsters persuading them to purchase high value/large quantities and send to the fraudster. We have issued a number of communications to raise network awareness and are supporting the Product Owner to explore options with Amazon and to strengthen current controls in Horizon by limiting the number of vouchers that can be sold/the amount or provide additional screen prompts for staff, currently solutions are being worked on, including timescales for delivery.
40. Following investigation into a suspicious activity report, we identified that high risk suspicious cash deposits from a Money Service Business (a money transmitter) were being accepted, via our bill payment reseller client Capita. Money Transmission is assessed by the National Risk Assessment as high risk for money laundering and such companies require enhanced due diligence. Our investigation of the deposits and activity identified that there was a complex structure involving numerous businesses between the customer and the end recipient, with some activity overseas and a similar structure to known money laundering typologies[2]. We are actively working with the Product Owner and Capita to cease the relationship with the businesses involved, and a meeting with Capita is scheduled for w/c 16th November 2020 to resolve. As a result of this case, we will work with the Product team to undertake a review of the existing contractual and control requirements related to Bill Payment re-sellers, and this will also form part of the Payzone

[2] In the AML/CFT context, the term "typology" refers to the various techniques used by criminals to launder money or finance terrorism

POL00423571

review.

Supply Chain Compliance

41. One of the 3 FTE has been off with suspected Long-Covid, which together with rising infection rates across the UK has impacted ability to undertake on-site assessments. A combination of remote checking, interviews, area manager interviews and site visits to low risk locations has been implemented.
42. The External Approved Contractor Scheme (ACS) assessment in October was completed remotely with only one observation identified. The score for ACS was assessed as 104, which is an increase of 10 from last year and maintains Post Office compliance within the top 5% businesses in the UK requiring this accreditation, indicating that despite the challenges over the last 7 months, compliance with ACS standards has improved.
43. An independent check of value stock picking accuracy at Swindon was supported. c.13% of one day's volume was checked and errors were identified in 1 in 109 items, despite the items already having been subject to a 100% operational check, i.e. the discrepancy had not been identified by the unit's own check. The outcome of the independent check has been escalated to Supply Chain and the Historic Matters Unit for them to remediate.

Financial Services

Multi Principal Review of 1st line controls (report expected January 2021).

44. Our three regulatory principals, Capital One, BoI and POMS, are undertaking a joint thematic review on the controls in place in the 1st line, including the work undertaken by the FS Compliance team. The scope of this work is far reaching and covers, 1st line controls over training, approvals, governance and compliance monitoring.
45. We are supportive of this review that will be a useful independent challenge and health check on our controls.
46. We will share any key findings with this Committee.

Compliance Monitoring

47. Mystery shopping had resumed on a small scale from August covering Over 50s cover and from the start of Q3 covering, savings and travel insurance.
48. Following the UK Government lockdown announcement on 31st October, with the agreement of our Principals who take compliance responsibility for our FS business, mystery shopping has been paused. It is expected in any case that sales of FS products will be reduced for the future period (for example TI sales will be very low/nil).
49. Following the approach of the 1st general lockdown we will use remote measures to review compliance performance. This includes quality of sales MI that reviews sales peaks, cancelation and complaints data. Our BAU governance with the regulatory Principals will continue so that any additional data from them (such as complaints made to the call centre) can also be reviewed.
50. For the mystery shopping we have undertaken this year the results from protection business have been generally good and within appetite. For Travel Insurance we will be using the small number of shops undertaken before lockdown to assess with POI whether any aspect of the revised sales process needs to be strengthened for future travel insurance sales when we can hopefully travel again.

FS Regulatory updates

51. A summary slide of the key future developments is included in the reading room at Appendix 8

POL00423571

3.

52. The government recently published a call for evidence on Access to Cash, which sets out the government's aims for protecting access to cash throughout the UK. It seeks views on:

    a. how the government can ensure the UK maintains an appropriate network of cash withdrawal and deposit-taking facilities over time through legislation, including the potential role of cashback;

    b. the factors affecting cash acceptance; and whether the government should give a single regulator overall statutory responsibility for maintaining access to cash.

    c. The Banking team will review the detail and decide how to best respond by the end of November.

Confidential

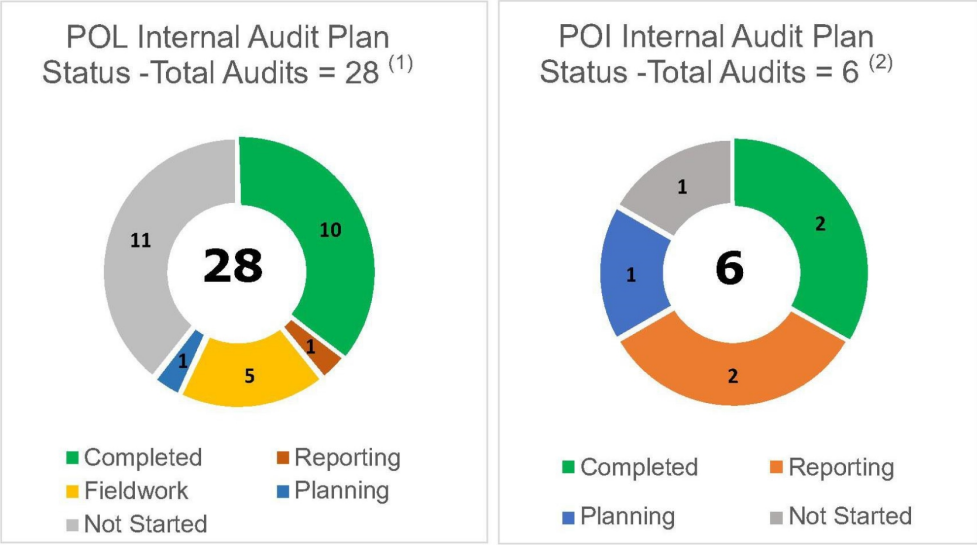
POL00423571

Internal Audit

Progress against Internal Audit plan

53. Delivery of the 2020/21 programme is making good progress, having completed five more audits since the September ARC meeting (4 POL & 1 POI).

54. Current delivery status is as follows:



(1)Target number of reviews based on revised plan for 2020/21 approved by ARC (18 Internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 9).

(2)POI ARC approved baseline plan for 2020/21.

55. A re-prioritised Internal Audit programme was approved at the May ARC meeting in response to Covid-19. It was agreed that a more dynamic (quarterly rolling) audit plan will be adopted and reviewed at each ARC. Further revisions to the plan was approved at the September ARC meeting and is included in the reading room (Appendix 9).

56. The following audits are being planned for delivery in Q3:

	Review	Sponsor	Timing	Status
1	Historic Matters (Post GLO) Set-up and Governance	Declan Salter	Oct	Reporting
2	Historic Matters (Post GLO) Operations Improvement Programme (Common Issues Judgement)	Declan Salter	Nov	Fieldwork
3	Mails & Parcels	Owen Woodley	Oct	Fieldwork
4	IT Controls Framework	Jeff Smyth	Sept	Fieldwork
5	Belfast Exit (Programme Assurance) Phase 2	Jeff Smyth	Oct	Fieldwork
6	PCI Compliance (Programme Assurance)	Jeff Smyth	Nov	Fieldwork
7	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Dec	Not started

Confidential

POL00423571

Internal Audit reviews completed

57. The following four POL audits were completed since the September ARC meeting:

1	Manual Revenue Adjustments		3	Identity and Access Management (JML) – Gap Analysis	
2	Effectiveness of Second Line during COVID-19 (Final Draft Report)		4	Branch Hub (Programme Assurance) (Final Draft Report)	

58. Our findings and observations from these reports are summarised below, with the full reports available in the reading room (appendices 5-8).

1. **Controls over Manual Revenue Adjustments** (Ref.2020/21-14)



Sponsor:
Al Cameron

Audit actions:

P1	0
P2	2
P3	1
Total	3

Appendix 5

In 2019/20 manual revenue adjustments made up £298m (31%) of reported revenue. At the May ARC, PwC raised a discussion point around manual adjustments to revenue made outside of Horizon, to ensure clients are billed correctly. Subsequently the ARC have requested that Internal Audit review the controls over this process.

The purpose of this audit was to provide assurance that the design and operation of the controls around manual revenue adjustments are robust and effective in mitigating the risk of error and consequential impact on Postmasters' remuneration. Our audit also assessed controls over transaction corrections, which may impact Postmaster accounts (c.127k corrections made in 2019/20 with a low average value of £37 per transaction).

We conclude that the control framework covering manual adjustment processes is comprehensive and well-understood by control owners. Whilst the preventative controls around review and sign-off are working well, there is an opportunity to further strengthen the detective controls with better explanations of variances and follow-up of aged items.

There is no direct link to, and therefore no impact on, Postmaster remuneration for the majority of revenue transactions processed directly in CFS. For the minority of transactions where Postmaster remuneration or accounts may be impacted, we found controls to be effective.

Management Comment provided by Tom Lee (Group Financial Controller)

"I was pleased to see the report confirmed my expectations, that a robust controls environment exists over what is an important and complex area of the business. The nature of revenue recognition across the organisation, driven by high volume of low value transactions with numerous interplays across systems and stakeholders, will inevitably lead to variances arising. The processes and controls in place are designed so as to keep these variances to a minimum whilst seeking to resolve those that do arise in a timely manner. We will continue to enhance this area and focus our efforts in the short term on the actions outlined within this report."

POL00423571

2. **Effectiveness of the Second Line during Covid-19** (Ref.2020/21-07)



Needs Improvement

Sponsor:
Nick Read

Audit actions[N1]:

P1	6
P2	15
P3	1
Total	22

[N1] Actions are included in the individual deep-dive audit reports and tracked through the normal audit process.

Second line functions in scope:
- CoSec
- Data Protection
- Financial Controls
- IT Governance
- IT Risk
- Central Risk
- Change
- Compliance [N2]
- Financial Crime [N2]
- Loss Prevention [N2]
- IT Security [N2]
- Health & Safety [N2]

[N2] Included in Phase 2 deep dive audits.

Appendix 6

The purpose of this audit was to consider the impact of COVID-19 on second line of defence functions across Post Office. This report covers twelve second line functions and consolidates findings from the interim report issued in July 2020 and three other deep-dive audit reports.

We conclude that during its response to the first wave of COVID-19, all second line functions **continued to operate** and are now better positioned to meet the challenges of the second wave. We also highlight the following **key successes**:

- Changes to processes and controls were made quickly but cautiously - often on a 'best-efforts' basis where the new arrangements were unprecedented.
- Management are monitoring the effectiveness of alternative controls adopted, particularly those brought about by branch visit suspensions.
- In response to the crisis, all functions have identified process improvements and intend to keep what went well.

We noted the following **areas for improvement** and ongoing challenges, which should be considered key learnings for the second wave of the pandemic and resulting regional and national lockdown restrictions:

- Vacancies and long-term absences mean at least three of the critical second-line teams cannot absorb additional demands without compromising effectiveness. Cost pressures mean some teams are operating at below pre-COVID resourcing levels.
- Restart of suspended commercial and technical development work, along with anticipated organisational change, could overwhelm second-line teams if not carefully managed.
- Lockdown fatigue - Good engagement with the business contributed to initial success, but some functions report that this is dropping off due to lockdown fatigue. This may worsen as we enter more regional and national lockdowns and adds to the pressures experienced by the second line.
- In some areas, clarity is needed of boundaries between first and second-line responsibilities, especially around process and control documentation ownership and maintenance.
- All second line functions faced increased risk, but the initial fall in transactions counteracted some of this. Risks may again increase during the second wave and may be exacerbated as Post Office enters the busiest time of the year.
- Controls are inconsistently managed. Some functions do not have documented controls and it is difficult for management to quantify the impact of their control decisions. Controls documentation was not always updated to reflect control adjustments.

Management Comment
tbc

Confidential

POL00423571

3. **Joiners, Movers & Leavers (JML)** (Ref.2020/21-01)	
 Needs Improvement ***Sponsor:*** *Jeff Smyth* Audit actions: P1: 1 P2: 0 P3: 0 Total: 1 A single overarching P1 audit action was agreed to update the current roadmap and action plan to include the gaps identified during this audit. *Appendix 7*	Internal Audit previously reviewed JML processes in 2017, identifying significant weaknesses in overall governance and the identification of JML triggers. Failures of JML controls have also been reported by the external auditors on numerous occasions. A JML Programme has been initiated by the business to identify and address control gaps and weaknesses, with regular progress updates provided to the ARC. JML controls were also covered within Cyber Maturity Assessments in 2019 and 2020, which showed a marked increase in maturity between the two reviews, with maturity targets being met for two of the four domains covering JML related controls. However, it is generally recognised that additional work is required to strengthen and automate access controls. The purpose of this audit was to validate the work undertaken by IT to support the business in identifying and remediating gaps in the effectiveness of JML processes and to assess the state of JML processes across the business, with the intention of ensuring only authorised users have access to POL systems. We conclude that IT have been making steady progress in addressing the JML control weaknesses. Considerable progress has been made over the last two years to enhance controls, through the implementation of SmartID, tying the creation and removal of user access to SuccessFactors, and introducing additional checks over access to key back-office systems. However, we observed a continued reliance on manual processes and insufficient coordination between teams responsible for JML, privileged access and vendor assurance. The roadmap and action tracker created by IT will support further improvements in JML processes and we have highlighted additional actions that should be included in the plan. We consider the residual risk of unauthorised access to POL systems to be substantially mitigated by the controls currently in place, but based on the actions still required, we have rated this report 'Needs Improvement'.
Management Comment provided by Tony Jowett (CISO) "This report is very timely and helpful in our quest to sort JML in Post Office. It re-emphasises that effective JML requires HR and IT to work closely together and the review of all in scope is very welcome. We agree with the action that we must create a roadmap/plan and would add an additional one about creating a picture of JML that could serve as a dashboard. Many thanks to IA for shining a light in this area."	

Confidential

POL00423571

4. **Branch Hub (Programme Assurance)** (Ref.2020/21-12)	
 Needs Improvement ***Sponsor:*** *Dan Zinner* Audit actions: P1 0 P2 6 P3 0 Total 6 *Appendix 8*	The 'Branch Hub' programme was initiated in 2018 to deliver a new digital self-service channel, to replace or support traditional channels for the interactions between postmasters and back-office functions. The overall delivery of the minimum viable product (MVP) and the adoption by Postmasters proved challenging, as noted in previous audits. In February 2020, the IC approved Branch Hub's move from the bespoke Fujitsu product to the ServiceNow platform. Due to COVID-19, the programme focused on delivering functionality to support Post Office's response to the pandemic, including 'Change Branch Hours', 'Agent Remuneration' and 'PPE Ordering'. This has driven adoption to surpass 9,400 users. The delivery of further features has been divided into three increments. As of August 2020, a total of £20.6m had been invested in the Programme. The purpose of this audit was to re-assess the operating effectiveness of programme delivery while ensuring previous audit recommendations have been adopted. Branch Hub has now demonstrated that it can deliver and that its underlying platform and delivery model are sound. Since its reset in February 2020, Branch Hub has been primarily driven in a short-term tactical way to prove it could deliver. This strategy was broadly successful as Branch Hub delivered its main objectives. However, it did not fully succeed in overcoming the inherent lack of trust and further constrained resources which resulted in some previous audit weaknesses not being fully addressed. We once again note that the programme lacks strategic direction and a joined up approach on how future features should be linked. GLO considerations have not been fully considered and embedded. We also noted additional controls weaknesses associated with the new delivery model. These gaps impacted on the overall programme performance, contributing to the present challenges in fully unlocking the committed FY20/21 benefits.
Management Comment provided by Dan Zinner (Group Chief Operating Officer) TBC	

Confidential

POL00423571

Post Office Insurance (POI) Audit Programme

59. The table below shows the status of the POI audit programme:

	Review	Timing	Status
1	Cyber Security (POL-POI Gap Analysis)	Aug	Complete (Sept ARC)
2	Incident and Breach Management	Aug	Reporting [N1]
3	Data Governance: Ethics, security and privacy • Phase 1 – Third Party Data Security • Phase 2 – Data Governance	 Sept Oct	 Complete Fieldwork
4	Special Investigation (Confidential)	Sept	Complete
5	Pricing: Principles, policies and process	Nov	Planning
6	Effectiveness of Risk Management – original plan	Q4	Not started
7	Channel review: Non-branch sales – original plan	Q4	Not started

[N1] This audit was delayed due to special investigations undertaken at management request and with POI ARC approval.

Status of Audit Actions

60. Audit actions are generally being completed on time. However, we highlight that the changes to business priorities due to Covid-19 have caused delays in completion of some audit actions. During May we worked with action owners and GE sponsors to agree revised completion dates for 14 actions impacted by Covid-19. Of these 11 have since been closed and 3 remain open and on track with the revised completion dates.

61. The movement and ageing of audit actions are shown in the table below (status at 05 November 2020).

Audit Action Status (POL):	
Open actions at last ARC	47
Less: Actions closed in period	31
Add: New actions in period	13
Total open actions	**29**

Ageing:	
Open (not yet due)	28
Overdue (<60 days)	1
Overdue (>60 days)	0
Total open actions	**29**

62. Following is a summary of the one overdue action and latest status update:

Description of audit finding and Priority rating	**GE owner and due date**	**Action Owners and Status Update**
Data Privacy (Document Retention)		
Finding (P2): Mechanisms for facilitating the deletion of records that are outside of their retention period are not defined (P2) Action: The CIO will work with the business to identify how record retention schedules will be operationalised to support compliance with the DPA and limit the time that personal data is held.	Jeff Smyth Original date: 30/04/2020 Revised date: 31/10/2020	**Owner:** Rob Wilkins The technical solution proved more complex than anticipated. Plans were underway to execute a Test and Learn process for IT to achieve implementation of automation of data retention schedules and to develop recommendations to create a business wide process for automation of data retention schedules. However, the action remains open. Further update provided in separate paper titled 'Data Management in Post Office'.

POL00423571

Appendices[3]

Compliance

Appendix 1: Communications Incident 2020 OFCOM Notification
Appendix 2: Telecoms Regulatory Calendar
Appendix 3: FS Regulatory Calendar
Appendix 4: Compliance Dashboard summary
Appendix 4a: Compliance Dashboard

Internal Audit

Appendix 5: Internal Audit Report – Manual Revenue Adjustments
Appendix 6: Internal Audit Report – Effectiveness of Second Line during Covid-19
Appendix 7: Internal Audit Report – Joiners, Movers & Leavers
Appendix 8: Internal Audit Report – Branch Hub Programme Assurance
Appendix 9: Internal Audit Plan for 2020/21

[3] Appendices are accessible in the Diligent 'Reading Room'

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE REPORT

Title:	PCI DSS Compliance	**Meeting Date:**	12th November 2020
Author:	Joseph Moussalli, PCI DSS Programme Manager	**Sponsor:**	Jeff Smyth, Interim Group Chief Information Officer

4.1

Input Sought: For Noting

The Committee is asked to note:

- What progress has been made during the last reporting period?
- What are the key risks?

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

The Risk & Compliance Committees (RCC) has requested a rolling update on PCI-DSS programme progress.

Executive Summary

The programme consists of 2 core delivery streams:

1. The Point-to-Point Encryption (P2PE) workstream, which encrypts retail and banking transactions from the Pin Entry Device (PED) to a PCI compliant zone in Ingenico before onward processing to Global Payments (retail transactions) or VocaLink (banking transactions).
2. The Target Operating Model (TOM) workstream which addresses use of PCI data by POL in processes outside of the transactions occurring at the PED.

Over the course of the last period, 2 key milestones have been completed culminating in the demonstration of a banking transaction going end to end between the PED and VocaLink. Additionally, we have completed accreditation of our payments solution and are scheduled to start a payments pilot through Global Payments on five counters in November

Overall the programme remains on track to begin a pilot with both payments and banking transactions in March. However, due supplier capacity constraints (in part due to COVID), it was agreed at the PCI programme steering committee that the Travel Money Card solution will be delivered as a subsequent release. Unless these constraints can be addressed, and more capacity becomes available, the timeline for a complete audit will move back to August '21.

The Target Operating Model workstream is progressing well and has progressed the secure solution needed for the Financial Crime team and a solution for processing BIN ranges greater than 6 digits.

Confidential

POL00423571

Key updates in the last period:

- PIN pad deployment has been completed. All branches have PIN pads ready for P2PE activation.
- Retail Payments:
  - Ingenico completed the Global Payments accreditation on 19th October 2020.
- Banking transactions:
  - Fujitsu, Ingenico and Vocalink completed the 3rd banking key milestone - a demonstration of a withdrawal from a POS located in the Fujitsu environment.
- Target Operating Model (TOM)
  - Financial Crime Team: Detokenisation application build has been commissioned with Accenture. This will be hosted on AWS by the Cloud Services team.
  - Release I (New): BIN>6 processing workaround has started.
  - Travel Money Card: Tokenisation solution agreed with FRES. Ingenico will need to activate tokenisation in the platform to support this requirement.
- Pivot to Cloud. Working closely with the Pivot to Cloud team to manage dependencies due to overlapping timescales.

- Finances: We envisage that there will be additional costs mainly due to the following factors:
  - Fujitsu overspend due to underestimating the complexity of the work.
  - New release approach – Travel Money card to follow as a standalone release that extends the duration of the programme by 2-3 months.
  - Covid-19 costs.
  - E-Portal / tokenisation.
  - Additional resourcing costs.

  The additional costs are currently estimated to be approximately £1.5m. The programme will firm up the costs and present these to the governance forums PRB, IC and Board once these are more well understood.

Questions addressed

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

Report

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

IT workstream

- PIN pad upgrade project was completed on schedule at the end of September. All PIN pads in branch are now ready for P2PE activation. The OBC contract is also in place for new branch openings and closings.
- The Fujitsu / Ingenico software development is tracking to our overall IT workstream plan.
- Payments Release: two interim milestones have been completed.
  - Payments release accreditation - Ingenico completed Global Payments accreditation on 19th October.
  - The Payments release has successfully completed UAT.

Confidential



4.1

- The Fujitsu Retail Payments pilot is on track to commence on 16th November 2020.

- Banking Release
  - Ingenico has delivered the 3rd key development milestone. This milestone provides a demo that a banking withdrawal can be made from a POS located in the Fujitsu environment using P2PE through to AXIS and Vocalink.
- POca – JPMorgan has completed the development of its migration to the banking framework.
- Good progress has been made with the Service contract with no major issues outstanding. This activity is now expected to complete governance and sign off in November 2020.
- A standing executive meeting now occurs every 6 weeks with Executives from both POL (Nick Read & Jeff Smyth) and Ingenico (Dan Martensson, VP Global Enterprise Sales & Regional Marketing, and Paula Felstead, Global CTO). Ingenico continues to provide commitment to achieve full accreditation with Vocalink by the end of January 2020.

Target Operating Model (TOM) Workstream Update

The focus of the Target Operating Model workstream is to review the Products and Processes that use Card Holder Data and to remediate and remove them from the scope of the PCI DSS audit where possible. If removal is not possible then PCI DSS controls will be put in place. A plan has been prepared to remediate the products and processes.

- An additional TOM release has been planned this period – Release I: BIN >6 digits workaround. Post Office products use BIN ranges greater than the six digits but the Ingenico product does not process more than six digits for PCI compliant systems. The Post Office team has worked with the business to adjust products and processes. However, a substantial workaround solution still needs to be put in place. This workaround is now being commissioned with Fujitsu, ATOS and Vocalink.
- High Level Solution Design HLD v2.6 has been approved by EAG. It includes the solution for Travel Money Card using Ingenico tokenisation. This solution has been agreed with FRES.
- Release A: Obfuscation of PCI data on screens and receipts. The solution has been developed and deployed into production.
- Release B: Telephone payments. The build has been deployed into production ahead of schedule.
- Release F (Quatrix): 14-day retention policy implemented on Quatrix. First Quatrix scan completed (14/08). Results indicate that there are no unauthorised processes using PCI DSS cardholder data. Mimecast (risk raised last month): A way forward has been agreed on how to implement alerting rules and a request has been made to Computacenter to implement DLP rules.
- Release G: PCI DSS compliant solution agreed with EAG for providing full PAN for the Financial Crime and Banking enquiries team. Accenture has been selected to implement the Ingenico detokenisation application that will be hosted in AWS.
- Release I (New): BIN>6 processing workaround. Work orders being agreed with suppliers.
- Success Factors: Support and Support Plus training modules were released onto Success Factors for Information Security and Data Protection to incorporate PCI DSS training requirements.

POL00423571

- Change Giving: Change giving has been confirmed as out of scope as Change Giving cards are not included within card schemes.

2. What are the key risks & issues on the programme?

The following are identified as key risks:

Risk: There is a risk that any changes needed to the Fujitsu/Ingenico software will impact the plan. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis of no further changes.
Mitigation: Post Office has managed to descope some of the changes identified by working with the business. At steerco it was agreed to implement two of the essential changes – BIN>6 processing workaround and Ingenico tokenisation. TMC could not be accommodated and so this will be delivered as a separate release. The steerco decision aims to keep the implementation of the P2PE solution for banking on track but there will be a delay to the PCI DSS compliance completion.

Risk: There is a risk that Santander cannot migrate services to route through Vocalink within the timescales.
Mitigation: Post Office team is working closely with Santander to produce proposals including costs and timescales. Santander has allocated resources to scope the work but this is running at a slow pace. The Post Office Director of Banking Services has been made aware of the issue.

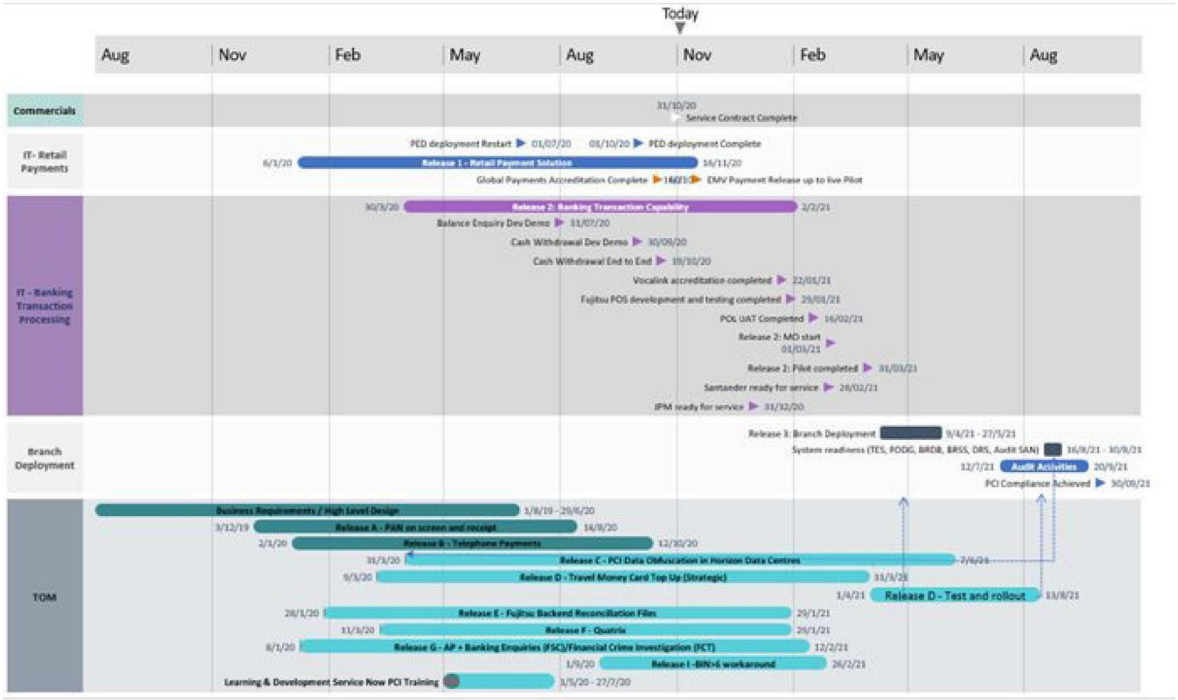
Risk: There is a risk that Coronavirus may impact the delivery timescales for any supplier across the entire PCI programme.
Mitigation: Post Office is working with all engaged suppliers to better understand their contingency plans to ensure that delivery momentum is maintained. This includes the examination of options to minimise delivery impact by understanding key delivery person risks, supply chain risks and other indirect or latent dependency factors.

Issue: Due to the complexity of the solution further funds will be needed. Fujitsu is forecasting an overspend of 10% - £504k; further funds will also be needed to accommodate the change in delivery approach.
Mitigation: Post Office has challenged the forecast overspend with Fujitsu and will continue to track and manage this issue. Further funding will be needed.

POL00423571

Appendix 1

Programme plan



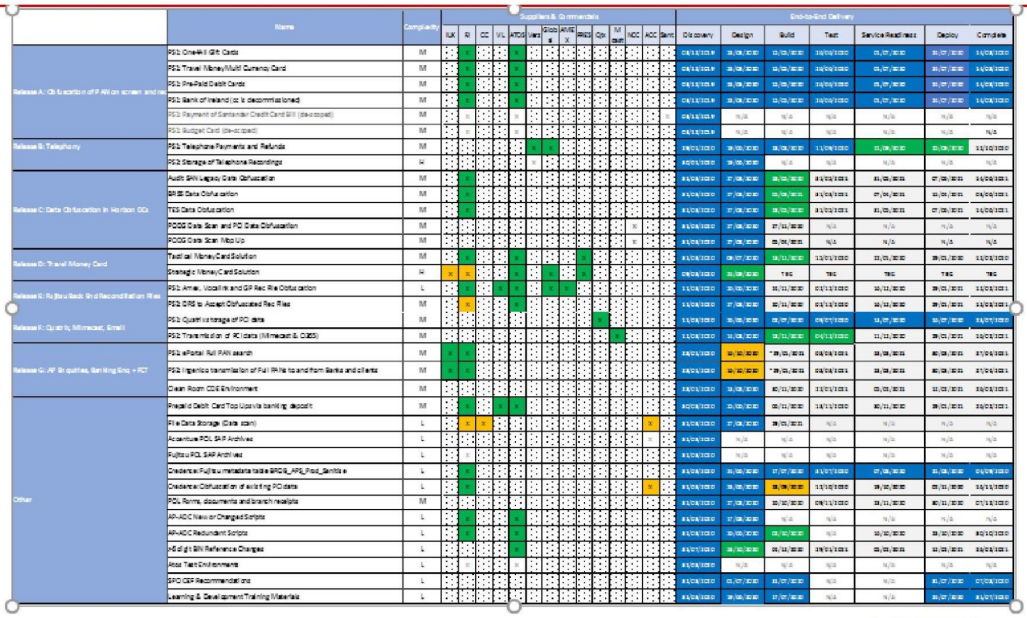
Confidential

POL00423571

4.1

Appendix 2

TOM Workstream Dashboard



	Name	Complexity	Suppliers & Commercials													End-to-End Delivery						
			ELK	RI	CC	VL	ATOS	Vero	Gisba	AIVE X	RMG	Qlik	M quit	ACC	ACC	Sent	Discovery	Design	Build	Test	Service Readiness	Deploy	Complete
Release A: Obfuscation of PAN on screen and rep	PS1: One4All Gift Cards	M		X				X									04/12/2019	28/08/2020	12/03/2020	16/04/2020	01/07/2020	31/07/2020	14/08/2020
	PS1: Travel Money/Multi Currency Card	M		X				X									04/12/2019	28/08/2020	12/03/2020	16/04/2020	01/07/2020	31/07/2020	14/08/2020
	PS1: PrePaid Debit Cards	M		X				X									04/12/2019	28/08/2020	12/03/2020	16/04/2020	01/07/2020	31/07/2020	14/08/2020
	PS1: Bank of Ireland (to b decommissioned	M		X				X									04/12/2019	28/08/2020	12/03/2020	16/04/2020	01/07/2020	31/07/2020	14/08/2020
	PS1: Payment of Santander Credit Card Bill (developed)	M		n/a			n/a										04/12/2019	n/a	n/a	n/a	n/a	n/a	n/a
	PS1: Budget Card (developed)	M		n/a			n/a										04/12/2019	n/a	n/a	n/a	n/a	n/a	n/a
Release B: Telephony	PS1: Telephone Payments and Refunds	M						X	X								28/01/2020	28/08/2020	28/08/2020	11/09/2020	21/09/2020	25/09/2020	12/10/2020
	PS2: Storage of Telephone Recordings	M						n/a									02/03/2020	28/08/2020	n/a	n/a	n/a	n/a	n/a
Release C: Data Obfuscation in Horizon DCs	Audit SAN Legacy Data Obfuscation	M		X													01/04/2020	27/08/2020	28/09/2020	01/03/2021	01/05/2021	07/05/2021	14/05/2021
	BRDB Data Obfuscation	M		X													01/04/2020	27/08/2020	05/09/2020	01/03/2021	01/05/2021	07/05/2021	14/05/2021
	TRX Data Obfuscation	M		X													01/04/2020	27/08/2020	28/09/2020	01/03/2021	01/05/2021	07/05/2021	14/05/2021
	POCG Data Scan and PCI Data Obfuscation	M												X			01/04/2020	27/08/2020	27/11/2020	n/a	n/a	n/a	n/a
	POCG Data Scan Mac Os	M												X			01/04/2020	27/08/2020	05/09/2020	n/a	n/a	n/a	n/a
Release D: Travel Money Card	Post oal Money Card Solution	M		X				X				X					01/04/2020	09/07/2020	18/11/2020	11/01/2020	11/01/2020	28/01/2020	11/02/2020
	Strategic Money Card Solution	M	X	X				X		X		X					09/04/2020	28/08/2020	TBC	TBC	TBC	TBC	TBC
Release E: Fujitsu Back End Reconciliation Files	PS1: Amex, Vocalink and GP Rec File Obfuscation	L		X			X	X		X	X						11/04/2020	28/08/2020	16/11/2020	01/12/2020	10/12/2020	28/01/2021	11/02/2021
	PS1: DRS to Accept Obfuscated Rec Files	M		X				X									11/04/2020	27/08/2020	30/11/2020	01/12/2020	10/12/2020	28/01/2021	11/02/2021
Release F: Quality, Mimecast, Email	PS1: Quantrix storage of PCI data	M										X					11/04/2020	28/08/2020	09/07/2020	04/07/2020	13/07/2020	31/07/2020	14/07/2020
	PS2: Transmission of PCI data (Mimecast & CIDS)	M												X			11/04/2020	28/08/2020	18/11/2020	04/12/2020	11/12/2020	28/01/2021	10/02/2021
Release G: AP Enquiries, Banking Enq + FCT	PS1: ePortal: Full PAN search	M	X	X													28/04/2020	30/10/2020	**28/01/2021	04/04/2021	12/04/2021	30/04/2021	07/05/2021
	PS2: Ingenico transmission of Full PAN to and from Banks and clients	M	X	X													28/04/2020	30/10/2020	**28/01/2021	04/04/2021	12/04/2021	30/04/2021	07/05/2021
	Clean Room CDE Environment	M															28/01/2020	28/08/2020	30/11/2020	11/01/2021	01/02/2021	12/02/2021	19/02/2021
Other	Prepaid Debit Card Top Up via banking deposit	M		X			X	X									02/04/2020	21/09/2020	05/11/2020	14/11/2020	30/11/2020	28/12/2020	30/12/2020
	File Data Storage (Data scan)	L		X	X											X	01/04/2020	27/08/2020	28/01/2021	n/a	n/a	n/a	n/a
	Accenture POL SAP Archives	L															01/04/2020	n/a	n/a	n/a	n/a	n/a	n/a
	Fujitsu POL SAP Archives	L		n/a													01/04/2020	n/a	n/a	n/a	n/a	n/a	n/a
	Credence: Fujitsu metadata table BRDB_APS_Prod_Santos e	L		X													01/04/2020	28/08/2020	17/07/2020	31/07/2020	07/08/2020	21/08/2020	04/09/2020
	Credence: Obfuscation of existing PCI data	L		X												X	01/04/2020	28/08/2020	28/08/2020	11/10/2020	28/10/2020	03/11/2020	10/11/2020
	POL Forms, documents and branch receipts	M															01/04/2020	27/08/2020	30/10/2020	09/11/2020	23/11/2020	30/11/2020	07/12/2020
	AP-ADC New or Changed Scripts	L		X				X									01/04/2020	27/08/2020	n/a	n/a	n/a	n/a	n/a
	AP-ADC Redundant Scripts	L		X				X									01/04/2020	30/09/2020	30/10/2020	n/a	30/10/2020	30/10/2020	30/12/2020
	6 digit BAI Reference Changes	L						X									01/07/2020	28/10/2020	05/12/2020	29/01/2021	05/02/2021	12/02/2021	26/02/2021
	Mac Test Environments	L															01/04/2020	n/a	n/a	n/a	n/a	n/a	n/a
	SPO CEF Recommendations	L															01/04/2020	01/07/2020	01/07/2020	n/a	01/07/2020	01/07/2020	01/08/2020
	Learning & Development Training Materials	L															01/04/2020	28/08/2020	17/07/2020	n/a	n/a	31/07/2020	31/07/2020

**Dependency on IT build, test and implementation dates

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

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

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

Confidential

POL00423571

Appendix 3 Finance Summary

The latest forecast below was presented to the latest PCI programme steering committee.

The financial forecast will be updated once the revised delivery plan has been firmed up and resourcing requirements have been confirmed. The table below now includes the Fujitsu overspend and additional costs for the known essential changes. We are still awaiting quotes for the remaining changes.

4.1

Once the costs are clarified, the programme will present the CR to governance at the earliest opportunity. The plan is to present the request for additional funding to the Board for review at its 26th January 2021 meeting.

PCI Programme Capex & Exceptional Spend (2018-2022)	Spend (to end Mar '20)	Actuals (Apr-Sep '20)	F/Cast (Oct'20-Mar'21)	F/Cast 2021/22	LIFE
Internal Labour	£142,589	£283,204	£321,388	£157,901	£905,081
External Labour	£1,016,232	£241,549	£385,866	£159,950	£1,803,597
3rd Party Costs	£3,727,554	£4,469,586	£4,002,564	£1,689,395	£13,889,099
Exceptional Costs	£115,000	£0	£0	£0	£115,000
Actual / Forecast	**£5,001,374**	**£4,994,339**	**£4,709,819**	**£2,007,246**	**£16,712,777**
3rd Party Costs Comprise					
Fujitsu	£1,955,216	£3,421,200	£2,335,043	£1,440,769	£9,152,228
Computacenter UK Ltd	£1,342,114	£415,886	£49,562	£33,794	£1,841,356
Atos	£202,011	£354,803	£490,174	£104,038	£1,151,026
Vocalink	£37,437	£131,728	£274,179	£0	£443,344
Other / TBC	£190,775	£145,968	£853,607	£110,793	£1,301,143
Actual / Forecast	**£3,727,554**	**£4,469,585**	**£4,002,565**	**£1,689,394**	**£13,889,099**

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4.2

Title:	Cyber Update	**Meeting Date:**	12 November 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with Cyber Security for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

Rolling item at each Committee.

Executive Summary

- We continue with our programme of work to develop higher levels of cyber maturity. This month we are focusing on the work to secure our AWS cloud-based migration of the Belfast Data Centre.
- We ran another fake-phishing attack with results that were very similar to those run in previous exercises. Strengthening of user education and HR measures may be necessary to make further gains.
- Our current cyber operations dashboard shows that phishing and data exfiltration from our network continue to be our main issues. More joint and across the board effort is needed to establish a cyber-aware culture.

Questions addressed

1. What is the latest update on the cyber programme with a focus on - what are we doing to ensure our move to cloud is secure?
2. What are the results of the recent fake phishing attack and recommendations?
3. What are the highlights from the current Cyber Operations dashboard

Confidential

POL00423571

Report: Programme Update and focus on how are we ensuring our move to cloud is secure for Belfast Exit?

4. The Status of the actions from the recent cyber maturity audit is as per the table below all are complete or on track within target dates

Finding	Status	Target Date
Target maturity levels for cyber security should reflect POL's risk profile	**Completed** – target maturity levels to stay as is unless risk appetite changes significantly	30/9/20
POL's list of crown jewels should be agreed with the business	**In Progress** – agreed list with CIO – to be agreed with GE/business	30/11/20
Security architecture is not fully documented	**In Progress**	31/12/20
There is no documented long-term cyber strategy	**In Progress**	31/12/20
There is no end-to-end programme defined for Cyber	**In Progress** – being developed in line with 20/21 planning cycle	31/3/21
The cyber action tracker requires updating	**Completed**	30/9/20
JML processes are not fully integrated	**Covered under JML paper** – requirement is to introduce automation of workflow where feasible	31/3/21
There is no documented strategy for Cloud security	**In progress**	31/12/20

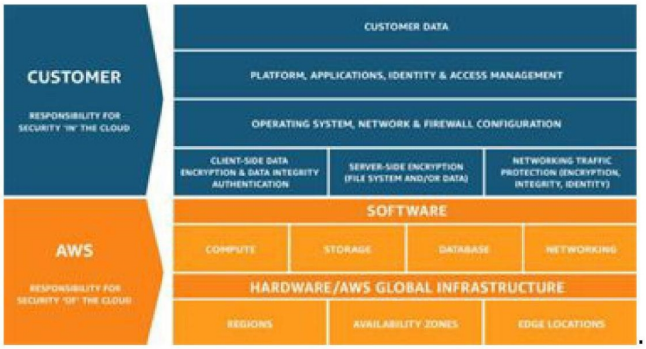
5. The roadmap for the cyber activity is show in Appendix 2.

Securing Cloud for Belfast Exit

6. As part of the Belfast migration a key requirement is, how do we secure the cloud and demonstrate we are at least as secure today if not more so in AWS than Belfast.

7. Firstly, we need to understand AWS public cloud offering. AWS operates a shared responsibility model between its customers and AWS; the below diagram illustrates where the responsibility sits for each organisation
    a. Post Office is responsible for all the services we consume and build on top of the shared software and hardware provided by AWS. **"We're responsible for security in the cloud"**
    b. AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services. **"AWS is responsible for security of the cloud"**

POL00423571



8. AWS responsibility layer removes the management and security responsibility of a physical data centre, therefore allowing the Post Office to focus time and recourses on protecting our digital environment without the burden of a physical location. AWS is certified to;
    a. ISO 27001 internationally-recognised standard for security management best practices and comprehensive security control
    b. Service Organisation Controls (SOC) 2 Report - evaluates AWS controls meet the criteria for security, availability, and confidentiality

How has the Post Office worked to delivery security?

9. Securing the cloud is a key responsibility of the CISO, the cyber security team has been integrated throughout the entire migration, managing the security delivery process;
    a. Ensuring the delivery of infrastructure & applications follows Post Office repeatable secure by design processes.
    b. Collaborate with AWS professional service consultants and trusted 3rd parties
    c. Implemented AWS Cloud Adoption Framework (CAF) which is AWS methodology for deploying securely into the cloud, focusing on the following security areas
        i. Identity & Access Management
        ii. Logging & Monitoring
        iii. Infrastructure Security
        iv. Data Protection
        v. Incident response
    d. Aligned Post Office Security Control Framework, based on NCSC (National Cyber Security Centre) 14 Cloud principles for alignment to the wider business.
    e. Conducted independent 3rd party IT Health Checks & Penetration tests on services delivered into the cloud.

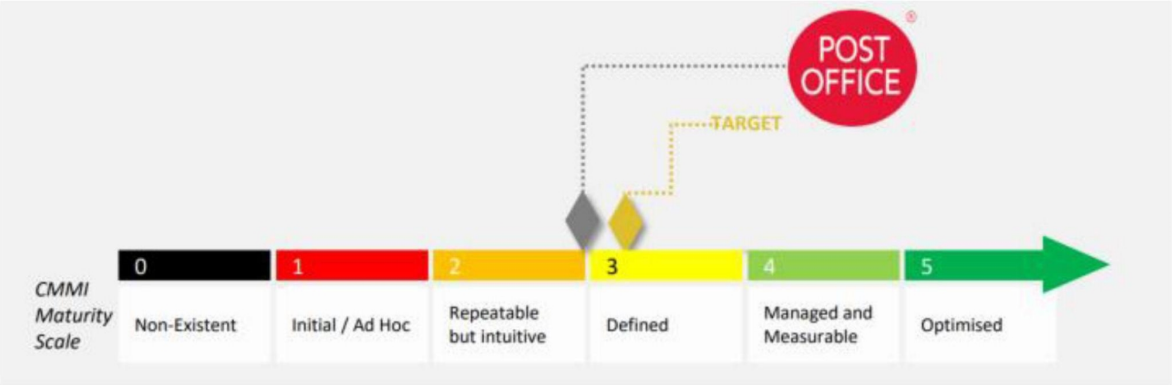
Cloud Security Maturity Assessment

10. We instructed a 3rd party to perform an independent cloud security maturity assessment Six months into our cloud journey to:
    a. Identify areas of strength in our approach to cloud security
    b. Identify current gaps in maturity and the resultant recommendations
    c. Define tactical and strategic objectives to improve maturity

11. We achieved an average score of 3.0 on the Capability Maturity Model Integration scale (CMMI) with a rating of Defined. Illustrating we have built a solid foundation with standardised repeatably processes, which will allow us to continue to mature.

POL00423571

12. Our set Maturity Target is 3.2 and is baselined against financial institutions and regulatory bodies, highlighting where these organisations are in their cloud journey.



Overall information security maturity rating for POL, alongside the overall scores of industry benchmarks.

Keys areas of focus for maturity

- Logging, Monitoring and reporting
- Privilege access management
- Security incident response
- Disaster recovery

Approach to ongoing security assurance

13. To obtain ongoing compliance to Post Office security controls – the security advisory framework has been established for each application migrating to AWS which includes;
    a. Design Review
    b. Security Control Assessment
    c. Risk Assessment
    d. Security testing, IT Health Check & Penetration testing, utilising internal tools or independent trusted 3rd parties
14. The above process will be tracked, and metrics provided once the migration starts to deliver further services.

Report: What are the results of the recent fake phishing attack and recommendations?

15. Phishing attacks are most used as successful forms of cyber entry point into an organisation. Using social engineering and phishing methods, cyber criminals rely on people to gain access to an organisation. This is orchestrated by delivering malware through emails as attachments or links which download malicious content on to a users' machine or the network when clicked. To mitigate, Post Office replicates real-life phishing simulation campaigns to understand the risk exposure and to educate colleagues.

POL00423571

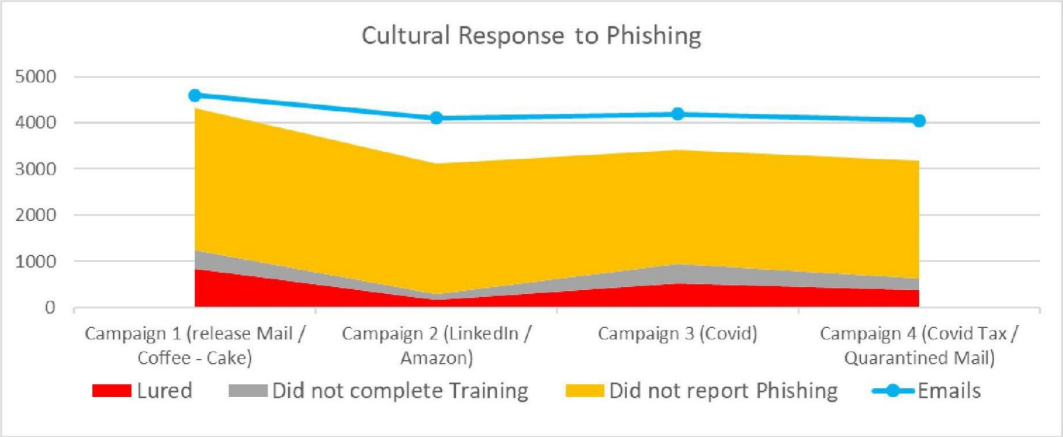
16. Our stats for a fake phishing campaign in October 2020 are shown below:

Emails sent	**4,047**
Total colleagues reporting as a scam	1,154
Total colleagues "lured"	*391
Post Office security measures initiated (average)	73 seconds
Total colleagues lured before mitigation	6
Skipped Training	178

17. For our defences to work correctly then we need users to report phishing emails rapidly so that others do not then receive the emails – the AI engines can only do so much and need user help to be accurate.

18. The two critical measures therefore are time taken for our security measures to recognise this specific attack as dangerous (73 seconds) and the number of colleagues who clicked or opened the attachment BEFORE these measures kicked is 6. This means that we could be dealing with 6 infected machines. Where payload from the attack included ransomware, then any one of those infections could result in a serious hit on our ability to operate as an organisation. The ransomware could have the ability for lateral movement and to replicate itself across Post Office.

19. Trends from all recent fake attacks shown in the diagram below:



20. Compared with recent fake attacks we have seen slight improvement towards reporting of phishing emails, but on average across all he fake campaigns about 45% will read phishing emails but not report it. Approximately 34% will report a phishing email. Approximately 17% of lured users who read and clicked the email, only 6% will commit to completing recommended training. This signifies a need to close the gap between people reading the email and those who report emails. Crucially for those who click on phishing emails, the gap between lured and training should be close to 0.

Confidential

POL00423571

21. Whilst there has been some improvement in the response to the attacks, they have not been material – meaning we have more work to do on the people aspects around phishing.

22. These stats show clear need for awareness across the business. As part of this we will be conducting, Cyber Lunch & Learn sessions to ensure our colleagues can ask questions about cyber in general. We will also explore with HR the potential for disciplinary action for repeat offenders.

23. Cyber will continue similar test attacks over the coming weeks and months – and we'll continue to report back the findings. We'll be starting a more regular pattern of communication over the coming weeks, to bring to life and highlight some of the tactics used by attackers, some of the more sophisticated patterns of attack and to provide advice for use both at home and at work.

Report: What are the highlights from the Current cyber dashboard?

24. Appendix 1 shows the current cyber operational metrics dashboard.

25. Key points to note are:
    a. Phishing attacks continue to risk albeit the rate of increase has slowed. We therefore need to continue with our work on fake attacks and user education.
    b. There are significant volumes of users that trigger DLP personal mail policy – again showing that we need to continue with user education.
    c. Change Assurance and Compliance trends demonstrate a reduction in net new actions, albeit activity within key programmes i.e. Belfast exit and PCI have increased. We expect a further up-tick in actions from the nascent SPM programme in the next few weeks.

POL00423571

Appendix 1

Threat Landscape (Cyber Perspective)



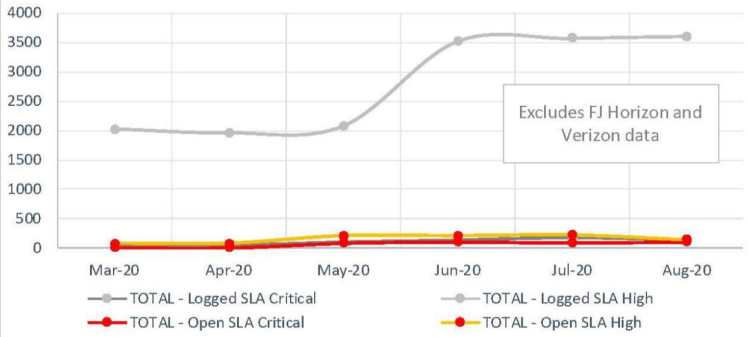
Security Posture



The existing controls are providing protection across all areas and IT Security visibility is increasing month on month, where controls are applied.

The SOC is consistently increasing maturity and handling an increasing number of threat scenarios, more so in recent months from Covid related, an increase in targeted phishing, an account compromise, alongside small data breaches and updated cyber risks have led to a minor reduction in posture.

Vulnerabilities (Accenture and CC)



CDP
- No Open Criticle Vulnerabilities

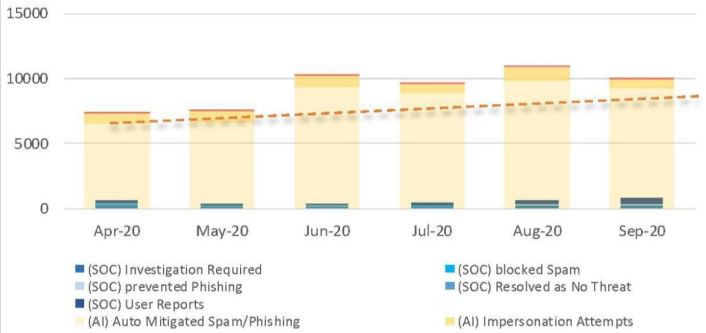
Fujitsu - Horizon
- Qtr3 scan due to be processed this October, Results due in Nomember Report.

Fujitsu - HPBB
- Replacement of vulnerability management tool Tenable started W/C 10th August 2020, Completion End Oct2020 ready for November Reporting

Accenture

A sub list of vulnerabilities not addressed, Accenture believe the process is being held up by POL (e.g. commercials etc.)
- Two critical vulnerability detected in SAP GUI (EOL/Obsolete Software: SAP GUI 7.40 and Earlier Detected)

Phishing Protection (AI and SOC)



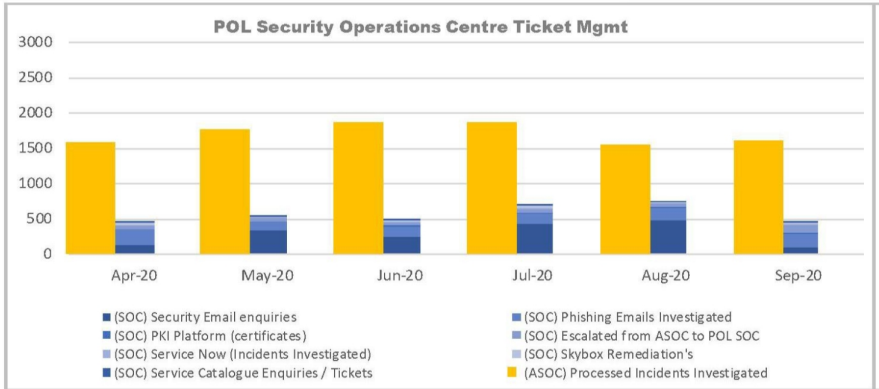
Trends indicate a flatlining of attacks albeit the trend is higher than this period last year. We are seeing more sophisticated attempts, with difficult to spot tactics being used across industry.

Early October an internal Phishing campaign was undertaken, results will be presented next period

AI - Artificial Intelligence systems contributing to 90% of Phishing remediation's which includes reports of phishing attempts by federated business. This is complimented by the Mail filtering (slide 2) systems on inbound mail that automatically remediate suspicious mail.

Confidential

POL00423571

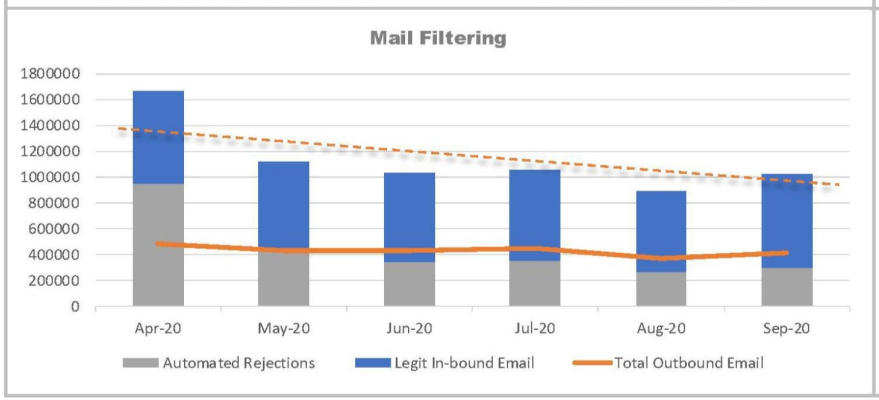


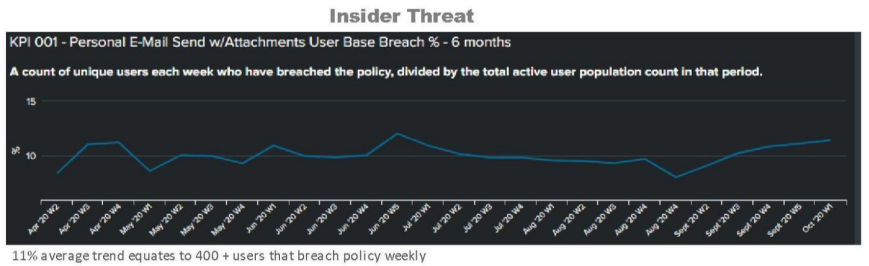
Cyber Major Incidents of note;

S2 - INC0281242 - User discovered personal image belonging to another user in desktop wallpaper profile, Incident was Investigated and identified as technical and process issue with Computacenter, handed over to Service Team.

S1- INC0281524 - corporate.postoffice.co.uk - Open access to the system was discovered during routine testing. Investigation results demonstrated that web hosting provider had failed in their controls and the engineering team had deliberately left a back door open to simplify change processes since March2020. Results also showed no data was compromised.

S1 - INC0280182 - Potential Data Exfiltration - Cloud Application Security intelligence System identified a user account that uploaded 800MB of data to a web data sharing site ('Sentry,io'). As a result of the investigation we have blocked the website/application, Anti Virus scans results show no malware found, Device Investigations found no sensitive data or malicious files. Possible credential sharing by POL staff.





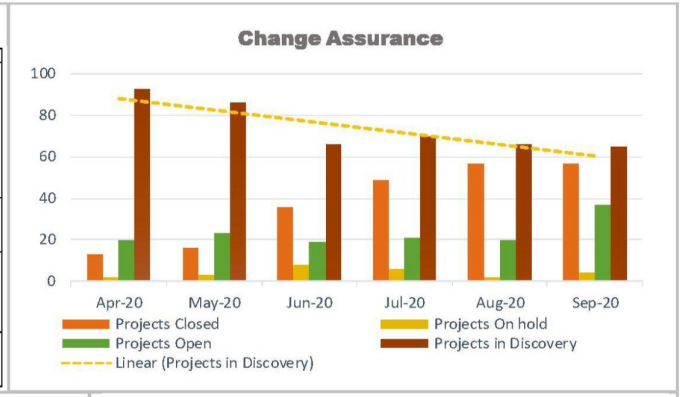
11% average trend equates to 400 + users that breach policy weekly

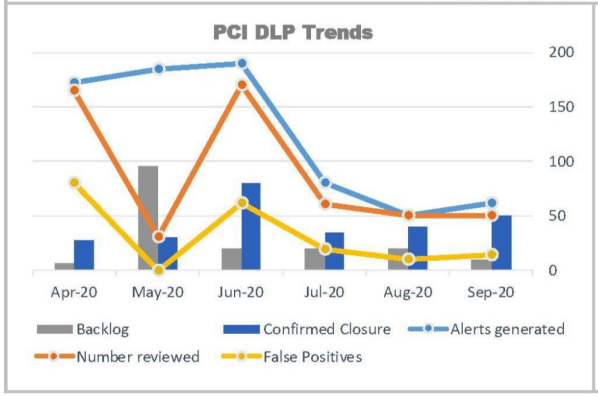
Confidential

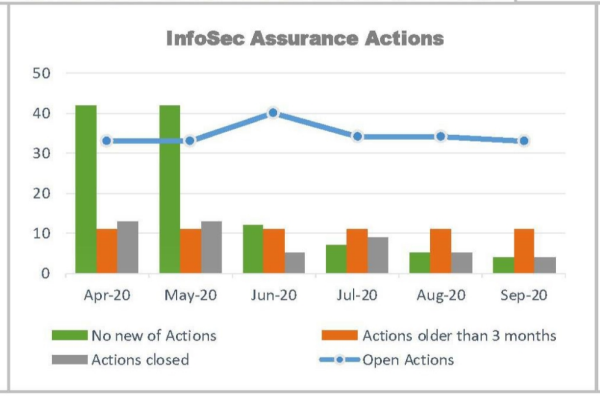
POL00423571

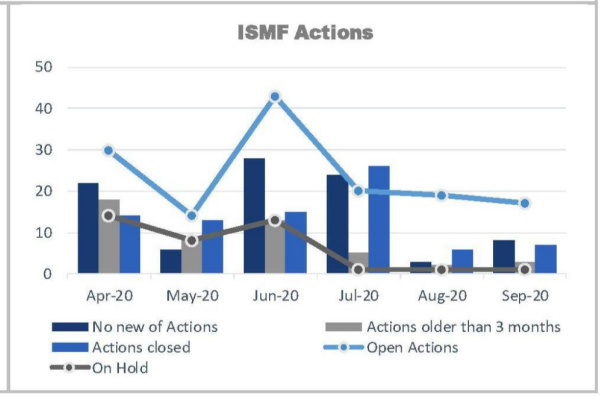
Covid-19 Tracked Major changes

Control/Policy	Change	Rationale
Password maximum age (expiry) of 90 days	This was extended to 120 days, although the complexity rules (3 out of 4 from upper/lowercase, numeric and special characters and certain "prohibited" combinations) remain in place.	Whilst this was initially implemented to avoid causing a denial of service to users whose passwords were about to expire, that requirement has been superseded by the implementation of the pre-logon VPN. The case can be made that enforcing a strong password and changing if less frequently (especially when people are working in a distributed way) actually enhances security as it reduces the tendency to write passwords etc. down. Consideration is being given to changing the policy and implementing multi-factor authentication to protect credentials that are increasingly valuable with the use of single sign-on. 25/09 – A change has been raised to evaluate the implementation of multi-factor authentication across the infrastructure (which will include LAN and Microsoft 365 environments). This will remove the reliance on the strength of passwords to protect all access. Once the options have been reviewed a decision can be made on whether to change the password expiry. 21/10 – Response now received from Computacenter for the discovery and design work. Workshop to be held later this month. It is intended to retain the revised password policy until global changes can be made across the authentication landscape.
Logon to laptop required before access to VPN is possible	The ability to initiate the VPN before local log on has been enabled in profiles on all devices. Multi-factor authentication is limited to the certificate on the computer.	Whilst this removes the need to share credentials for users with new devices, it makes access to the VPN slightly more open. The use of multi-factor authentication will be evaluated in conjunction with the Active Directory credentials above. 25/09 – The implementation of multi-factor authentication (above) will mitigate this risk. 12/10 – This will be rolled into the multi-factor design being dealt with in the Computacenter response above.
Only on premises AD-joined devices allowed to access the infrastructure	The pilot Intune managed Windows 10 devices have been permitted access as corporate devices joined to Azure AD.	This is the way all devices will be managed going forward, "Modern Management" via Intune is the strategic approach. Configurations have been developed which provide comparable security controls, and processes for the review and monitoring of these are being developed. 25/09 – The controls on the pilot Windows 10 devices continue to be monitored, but the restrictions on local saving and use of web clients places them at no higher risk than the non-POL devices that are permitted access under the BYOD usage policies. 21/10 – This is being held in abeyance until the EUC strategy is known and migration from the existing Windows 8.1 platform takes place. The pilot continues to be refined; and is planned to be the model for management of Windows 10 devices once migration takes place.
All testing on Horizon equipment is undertaken from physically secure supplier locations	Testing of Horizon changes to be undertaken on existing devices moved to Atos and CC users' homes	Although access to conventional testing locations is no longer possible where strong physical controls are in place, devices are secured by process/guidelines. This remains in place and is facilitating the continued testing for releases. 25/09 – This has continued to be monitored, with no incidents being recorded. The arrangements are being reviewed in the context of the Atos 21/10 – A similar arrangement is being put in place for testing to be undertaken by Ingenico for the P2PE project with similar processes and guidelines





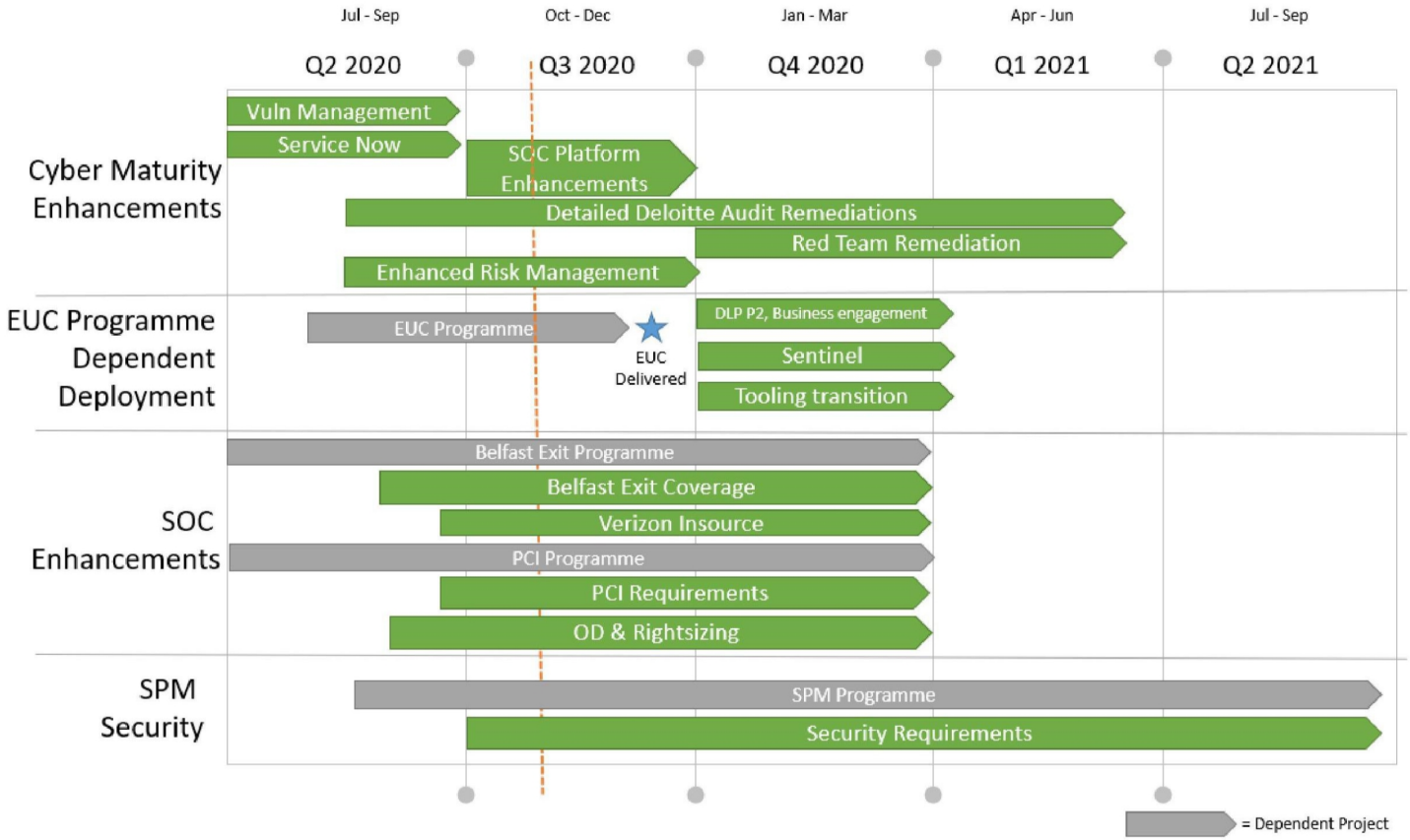




Confidential

POL00423571

Appendix 2 –2020/1 Cyber Programme



Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4.3

Title:	Joiners, Movers, Leavers Update	**Meeting Date:**	12 November 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML) – in particular those associated with Movers during the current hybrid operating model, for onwards submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

Actions to report on this occurred at the previous Risk and Compliance Committee (RCC) meetings.

Executive Summary

In our continued focus on Joiners, Movers, and Leavers we have performed a deep dive on the Movers process, following on from the previous report's focus on Leavers. Our analysis covers a period for which COVID-19 continues to be actively changing our operating model and introducing new challenges. Short term and longer-term actions are included for movers and an update is provided on the actions raised in the previous paper.

In addition, we have worked closely with Internal Audit who have reviewed JML across the business and IT platforms. In line with this review we are drawing up a roadmap and plan for improving JML within Post Office to give further clarity on dates, achievement, and operationalisation of good JML practices.

Confidential

POL00423571

Questions addressed

1. What are the complexities that we need to address associated with the Movers process?
2. How well have managed those complexities during the period July-September 2020?
3. What progress have we made on the actions identified in the last paper?
4. What are the key points and actions arising from the IA audit of JML?
5. What are our next step

Report

1. In this report we are focusing in on the Movers process for staff and contractors as this presents the next greatest risk to the business to Leavers and is a process that is likely to be tested during the current and future Organisation Development activities.

What are the complexities that we need to address associated with the Movers process?

2. Effective moving of role in POL is reliant on that the old- and new-line managers informing People Team and IT what is happening and what corresponding data access is required. Guidance is available for line managers with a detailed checklist on the Post Office Intranet and People Team business partners reinforce this process.

3. For any Mover the ideal behaviour is that the access rights associated with the old role are dropped and then rights are created in line with the needs of the new role.

4. The Movers process needs to cope with the different types of mover covering at least:

    a. Formal role move resulting from a vacancy being made available, interviews and job award
    b. Formal secondment for up to a year from a substantive role
    c. Informal secondment to cover a temporary absence or gap

5. There is a heavy reliance on line management in Post office to run the movers process. Informal and Formal Secondments do not get tracked routinely on Success Factors – - they only appear if line management remember to do it. Likewise, any associated changes to IT data access – they only get changed if line management remember to do it.

6. Good movers practice would also be backed up by a periodic data recertification activity that would pick up an movers data access that was incorrect.

How well have managed those complexities during the period July-September 2020?

7. People Team do not routinely produce a report regarding movers in the same way they do for leavers. The lack of such a report also means there is no routine oversight or auditing of this process. Success is therefore heavily dependent on line managers doing the right thing at the right time.

POL00423571

8. The People Shared Service Centre (PSSC) were able to produce a custom report showing those whose role title had changed and from this a subset of people who were movers was identified manually. By this analysis there were 34 people who had moved role during this period - on average one every other day.

9. For each of those 34 people a check was performed with IT service desk to see if any data change requests had been made by line management – as per guidance on POL intranet. The IT service desk confirmed that no such requests had been received for these individuals from anyone.

10. In the end user computing environment data recertification checks are not performed or coordinated centrally – they are reliant on individual data owners doing their own checks as and when they deem it necessary.

11. The recommended improvement actions are:
    a. PSSC to produce a monthly mover's report (like the leavers report) to go to each GE area for confirmation by line management and to go to IT Service Desk (Target Jan 2021)
    b. IT Service to develop the ability to automatically drop a mover's access and create new access in line with the new role (Target Jan 2021)
    c. Develop a fit for purpose data recertification mechanism to catch any inappropriate data access (Jan 2021)
    d. People Team to continue with efforts to move PSSC to Service Now enabling case management across People Team and IT (previously identified action - dates as per roadmap/action plan and in progress with approvals)

What progress have we made on the actions identified in the last paper?

12. In the last paper we identified a series of actions around JML. Of these 11 were due by end October.

13. Of the 11 due for completion
    a. 6 have been completed
    b. 4 are in progress with estimated completion dates in November. These are
        i. Recruitment of JML/Controls analysts x 2 – we are searching for suitable candidates
        ii. Production of GE leavers report - with PSSC to produce draft report
        iii. Privileged access additional approvals by CIO/CISO (feasibility being investigated with PAM team),
        iv. Spot auditing of 3rd parties where we currently have attestation only (resource offered role and starting in December)
    c. 1 pending PRB approval (PSSC move to SNOW)

Confidential

POL00423571

What are the key points and actions arising from the recent audit of JML?

14. An audit of JML by Internal Audit (IA) has just been completed with a report to be presented at this meeting.

15. The purpose of this audit was to validate the work undertaken by IT to identify and remediate any gaps in the coverage of JML processes and to assess whether these will address the requirements for all user types across all platforms.

16. A summary of the high-level findings of this report and an initial response to them is below:

Key Finding	Response
POL have undertaken considerable work to address concerns around JML over the last two years. This includes the integration of SuccessFactors and AD via MIM and increased review and monitoring of access to back office applications by the Data Services Team. Many controls continue to require manual intervention and IT should help identify methods to enhance automation across the JML estate. The planned integration of JML processes on ServiceNow will help to address this issue.	This finding is accepted and was previously identified as an action. People Team are currently developing the business case to move the People Shared Service Centre to Service Now.
Controls in place over access to Horizon and AD provide mitigation against the risk of unauthorised users accessing POL systems, however further work is required to ensure that starters and leavers are identified in a timely manner, to limit any sharing of IDs (Horizon), and to support monitoring and recertification of user accounts, especially those with privileged access, across all platforms.	Noted and specific actions are included in the JML plan
IT have taken responsibility for identifying and tracking actions required to further enhance JML processes and we have identified actions which should be included in the roadmap and tracker within this report. Responsibility for the operation of JML remains the responsibility of all POL staff and there is a key reliance on Line Managers to perform their duties in respect of JML effectively	Noted – further activity is needed to be clear on the parts of JML which are owned by People Team, IT and other areas of the business. The Line Managers role in this could be strengthened by further oversight of the end to end process – actions to be included in the JML plan.
The audit has a single finding namely - Create a roadmap and action plan and update to reflect points identified in this review.	Noted and first draft in development. The actions from the audit and other actions are being consolidated into a single plan.

POL00423571

Next Steps

17. Whilst the IA audit findings are being presented and discussed by RCC and ARC in parallel we are developing:
    a. A combined JML road map and dashboard to make it easier to track and communicate progress (January 2021)
    b. A combined detailed action plan
    c. A dashboard covering the whole of the JML universe status within Post Office
    d. An augmented team to accelerate the delivery of improvements covering business analysis, SME input and coordination across PO group (subject to PRB funding approval)

18. We are commencing planning with PWC on the PWC IT audit as part of our financial audit activity which has JML actions.

19. In the next paper

    a. We will review joiners activities for end user computing.
    b. In line with the new purpose of being there in person for the people that need us we will also assess the Horizon JML regime. We will specifically focus on ensuring that account sharing is limited and resiliency of the access management platform to ensure that our new purpose is fully supported.

20. We will continue to make progress on the actions previously identified from the previous paper that are due in November and complete those that are in progress from October.

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4.4

Title:	Briefing on August Belfast data centre Disaster Recovery	**Meeting Date:**	12 November 2020
Author:	Gary Walker, IT Director	**Sponsor:**	Jeff Smyth, Group CIO

Input Sought: For Noting

The Committee is asked to note the follow on plan regarding the Belfast datacentre disaster recovery test.

Executive Summary

1. The Fujitsu Belfast datacentre currently hosts Horizon and other business critical applications used to deliver branch counter services. Disaster recovery failover testing of the estate is due annually. The previous test was performed in October 2019 and for 2020 the test date was agreed as August 29th 2020.

2. In 2019 the original test was to fail over on Saturday evening, deliver services from the disaster recovery secondary site on Sunday, then fail back Sunday evening. This test failed and a plan was put in place to remediate and re-test. This re-test was completed in October 2019 but with a reduced test scope carried out over only one night which was successful.

3. For 2020, it was agreed that in addition to the original failover and failback plan from 2019, we would run services for a full day of trading in the secondary (disaster recovery) site before failback to the primary Data Centre.

4. During the 2020 test, failover to the secondary datacentre was completed within 4 hours but this was 2 hours behind schedule due to a delay in failover of core networking components. Fujitsu (post-test) subsequently completed investigation into the root cause and mitigating actions have now been implemented.

5. Testing during failover resulted in 48 of the 51 tests completing successfully. There were three Services which did not pass testing: (i) Debit Card transactions via the TNS service, (ii) Telecoms and (iii) National Express transactions. Due to the 2 hour delay in failover, there was limited time to troubleshoot the failed tests. As Debit Card transactions were deemed a critical service for trading a decision was made for trading on Sunday on the secondary environment to be abandoned and failback to production. This was to ensure that all services would be available for start of day on Sunday.

6. The risk position is considered to be unchanged following this test as subsequent to the test Fujitsu have investigated and implemented mitigated for all failed components.

Confidential

POL00423571

7. Four options are available as part of our next step actions and one of these has been recommended which is to complete only failed component testing and defer wider testing to an appropriate point in the Belfast Exit programme

Questions addressed

- What is the result of the 2020 failover test?
- Has the test altered the risk position?
- What are the next steps?

Report – What is the result of the 2020 failover test?

8. Due to Covid the test was deferred from the early part of the year which required a reasonable amount of re-planning. The planning for the test commenced 10 weeks before the test date, working with key business stakeholders and partners. Model Office were fully engaged to ensure full regression testing across the platform. No major obstacles were encountered in the planning however it was challenging to get full Business User engagement for testing across all the services in scope.

9. A POL change freeze was implemented to take effect just prior to the event, but some confusion ensued as this was out of alignment with Fujitsu's change freeze. Better alignment on this matter is needed in future and it has been noted as a lesson learnt.

10. Pre-failover baselining was completed successfully on Thursday and Friday (27th and 28th). All Go/No Go stage checkpoints were attended by IT Senior Stakeholders, Business Representatives, POL Test Teams and partners. No blockers to a Go decision was voiced on any occasion and Failover commenced as planned 19:00, Saturday 29th. A Gantt chart showing progress versus plan is shown in the Appendix 1.

11. The comms plan was executed well with good communications and effort throughout from all parties and partners. However, three Clients (Santander, Camelot and GlobalPay) reported issues during the planned outage. It was subsequently confirmed that they had been properly informed of the test timelines and impact, but they had not passed on this notification internally. Positive confirmation from all partners has been added as a lesson learnt for future tests.

12. Call bridges worked well with timely attendance noted and helpful input provided by all as needed. Hourly reports were produced via Horice as an aid to monitoring stability and availability during the execution of the test which provided an active view of the entire transactional state across all branches and counters.

13. The plan expected the Core Services (banking) to be available at approximately 23:30. Despite being approximately 30 mins ahead of schedule early in the plan Fujitsu informed us at 22:38 that we were no longer ahead of schedule due to key network components taking longer to failover (network stabilisation issue).

POL00423571

14. At 23:30 Fujitsu informed us that that they were now running 1 hour 10 mins behind due to further restarting of underlying infrastructure to rectify the network stabilisation issue. A follow up review was scheduled for midnight.

15. At 00:00, Fujitsu indicated the ETA for Core Services was now 01:30. The progress was monitored closely, and core services were made available at 01:00.

16. After some initial slowness, testing commenced with notable results which included Banking services being tested successfully at 01:30 am.

17. Testing of all other services commenced testing at approximately 01:45 where it was reported that (i) debit card (TNS) transactions were not working. Two further test failures occurred for (ii) Telecoms and (iii) National Express were reported.

18. The delay in the failover of data centres (due to the network stabilisation issue) resulted in very limited time to diagnose and correct any issues by the 'point of no return' deadline of 2:30 am, at which point the decision had to be made to fail back or remain in the secondary disaster recovery site for Sunday trading. As no fix for the Debit card issue was imminent, at 2:15 the decision was made to fail back to the primary datacentre to ensure full service availability for Sunday trading.

19. The failover back to the Primary Data Centre was very successful being completed ahead of plan by 1.5 hours, with no issues (see Appendix 1). The majority of batches completed successfully with no processing issues found. Two files sent via the PODG (Post Office Data Gateway) system were delayed by approximately one day due to the nature of how they are created (they require input from other 3rd parties). It was agreed that deeper analysis of impact to PODG should be done in future to allow better communication to processing parties in future tests. This has been noted as a lesson learnt.

20. Horice was utilised on Sunday to double check that all transaction types were completing successfully with volumes within normal Sunday trading levels.

21. Fujitsu agreed to perform full root cause analysis, evaluate and to advise in due course with the expectation that remediation will be made as needed. At the time of writing this report, the root cause of all failed elements have been rectified.

22. Post Test Weekend Observations and Comments have been documented in Appendix 2.

Report – Has the test altered the risk position?

23. Overall it is considered that the Fujitsu risk profile has not changed materially as a result of this test. 48 out of 51 Services did (functionally) failover and all services failed back and were successfully tested. During the failover, test transactions done in Model Office were successfully replicated to the secondary site and evidence could be seen of these being stored successfully on the Horizon database. Though the test cannot be considered 100% successful, the failed components would not prevent POL from being able to meet key service delivery obligations in response to a disaster.

24. The Current Risk Score is 6 (Medium) and remains so due to the following 2 factors:
    - Full Days trading Volume in secondary datacentre not tested

Confidential

POL00423571

- Data replication of full day's trading from secondary back to primary datacentre not tested, however, evidence of data replication was seen as a result of model office testing (this proves the mechanism but not the ability to cope with a full days transactional load)

Report – Next Steps

25. There are four options available to us with regards to further risk mitigation (if required). Our recommendation and current plan is to proceed with **option d**:

a) Assurance of Failed components

Do not conduct a full failover again but seek to verify the 3 components that failed in isolation. This will provide confidence that the components that failed have been corrected. This gives nil cost impact as these activities can be tested in BAU. There will be only minor interruption to BAU during testing. Note that 2 of the 3 components were successfully tested in October after having the root cause of failure fixed.

b) Failover to secondary disaster recovery site, re-test failed components only

Conduct the failover again, but only retest the remediated components and then fail back. We would not plan to run for the day in the secondary disaster recovery site. This provides only marginally more risk assurance than option (a). Estimated cost of £40,000 with expected outage to business of 8 hours over a Saturday night. Given proximity to peak period, this would need to be done in 2021 but with close liaison with the Belfast Exit programme as the underlying estate is fundamentally changing as this programme continues to execute.

c) Repeat the full disaster recovery test, with initial scope to remain in IRE19 for full day Sunday trading

Repeat the test with the full scope, including running on the secondary disaster recovery site for a day. This would provide full assurance that disaster recovery is but would be disruptive to the business as well as carrying the highest cost. Estimated cost of £80,000 including additional supplier support and Project Management resource to run the event. Expected outage to the business would be 4 hours Sat night, 5 hours Sunday night and potentially more. Given proximity to peak period, this would need to be done in 2021 but with close liaison with the Belfast Exit programme as the underlying estate is fundamentally changing as this programme continues to execute. The next appropriate long weekend would be over Easter.

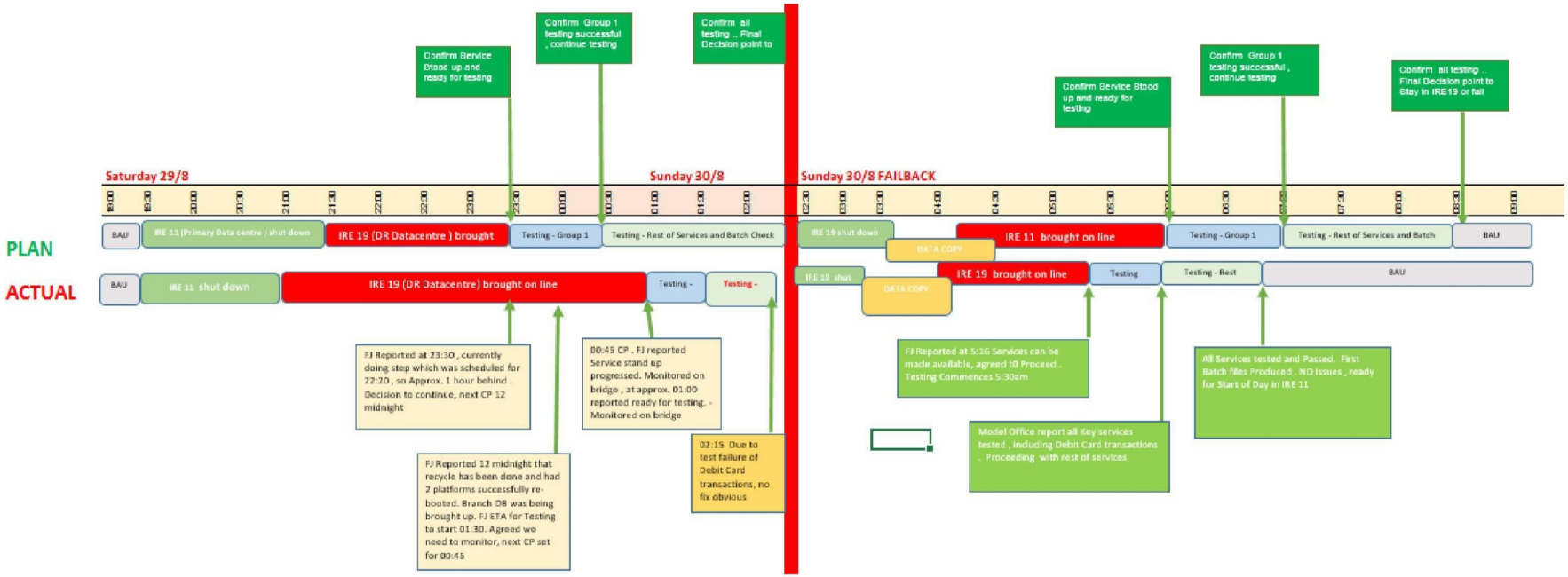
d) Complete only failed component testing and defer wider testing to Belfast Exit

Verify the 3 components that failed in isolation after remedial activity is undertaken (option a), then move the scope of the wider disaster recovery test into the Belfast Exit programme of work to occur once the virtual datacentres are ready. Once ready, run an equivalent disaster recovery exercise. There would be no cost impact as this activity is already covered under the Belfast Exit programme. However, the exercise will look materially different to the existing physical test as the majority of services will be resilient by design and therefore will only need limited testing

POL00423571

Appendix 1

Plan 'V' Actual for Key Activities during the event . Moved to Failover plan at 02:15 Sunday Morning



Confidential

POL00423571

Appendix 2

Issue / Observation	Next Actions	Estimated Resolution Date
We need assurance of the debit Card (TNS) service in the secondary disaster recovery site	Fujitsu to present plan for testing this is isolation	October 2020 [COMPLETE]
Services for recovery are grouped into a two-tier priority order. It was mentioned that priority review for each service should be made to assure recovery smart recovery order (such as for Debit Card usage moving to tier one)	Review Contractual Obligations on failover, and re-align	November 2020
Slow service/network performance was noted immediately after failover. It was suggested this might be due to the load that many branches registering would generate.	In subsequent Counter Outage (done Monthly) test to see if same behaviour exists in primary Data centre	October 2020 [COMPLETE]
Fujitsu mentioned that their Application Support team would like to work directly with Model Office to get a deeper understanding on what is tested and test scripts etc. with a view to offering to better manage and predict service performance throughout a test which may aid more immediate diagnosis on issues and earlier trouble shooting	Revised Model Office Script to be shared with Fujitsu to enable them to create matching diagnosis scripts	November 2020
PO require greater visibility of what is being tested before handing over to PO, i.e. what connections had been checked and Verified before handing over for testing. This could result in faster mitigation, for example with the TNS issue experienced this test.	Fujitsu to compile list of checks that are performed prior of handover to Post Office	October 2020 [COMPLETE]
Test plan need to be reviewed to ensure all service are included, e.g. BG, pay point as they were not included in this test.	Model Office plan used needs to be reviewed to include any other required services	October 2020 [COMPLETE]
A next test requirement was suggested to isolate access to Model Office counters only before opening systems to all Branches	Fujitsu to build into test plans, ready for any subsequent disaster recovery test	Nov 2020
Evaluation of Belfast Exit implications for further testing should be made. As Belfast Exit continues and scope changes, failover scripts will need ongoing constant refinement	Belfast exit Program with Fujitsu and Post Office IT to review Belfast Exit Programme to understand feasibility of conducting further disaster recovery tests during exit programme	Nov 2020

Confidential

POL00423571

Future state disaster recovery testing options from Belfast exit need to be understood and considered so as due testing is made at appropriate points during that transition	Belfast Exit Programme to report on how disaster recovery assurance can be maintained during the exit programme.	Nov 2020
Their was some confusion on the change freeze that was put in place due to different communications from Fujitsu and Post Office. Alignment and clear guidelines on change freeze requirements required going forward	Future Change Freeze Requirements to be aligned with partners and shared appropriately	October 2020 [COMPLETE]
Some third party operational teams raised issues during the outage period due to the change . Third parties had been informed , but it was found this had not filtered down to the operational teams. Positive confirmation from all partners that this is done will be required.	In future planning , positive confirmation that the outage periods have been communicated with all operational teams will be required	Nov 2020
There were some unknown delays to a couple of PODG file deliveries. It was found there was a lack of detailed knowledge required to assess full impacts of these files when planning was done	A deep dive into PODG routes and impacts to outages is required and hence be communicated for future tests	Nov 2020

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	The Historical Operation of Suspense Accounts	**Meeting Date:**	12 November 2020
Author:	Mark Underwood, LCG Operations Director, Tom Lee, Financial Controller & Tim Perkins, Head of Security, Safety & Loss Prevention	**Sponsor:**	Ben Foat Group General Counsel & Alisdair Cameron, Group Chief Finance Officer

5

Input Sought:

The Committee is asked to note the findings from KPMG's review of Post Office's historical operation of suspense accounts for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

- Post GLO Settlement Programme SteerCo of 1 July 2020.
- Risk & Compliance Committee (RCC) and ARC of 13 July and 27 July 2020, respectively.

Executive Summary

1. Allegations continue to be made that Post Office may have recovered sums from Postmasters which were not 'real losses' to Post Office as they were housed in suspense accounts and taken to profit by Post Office.
2. KPMG were instructed to review Post Office's current operation of suspense accounts. Given the robust and transparent investigations process that is undertaken, their principal finding was that how these suspense accounts are operated today should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit (nor had any evidence been presented to indicate this had happened).
3. The ARC approved instructing KPMG to also review Post Office's historical operation of suspense accounts. This review involved looking at two suspense accounts - the Agent Creditor Suspense Account and the Customer Creditor Suspense Account.
4. The Agent Creditor Suspense Account. From their review of historical practice, KPMG has found no evidence to suggest that amounts posted to this account relate to discrepancies which should have been repaid to Postmasters.
5. The Customer Creditor Suspense Account should only include sums that relate to outstanding / unmatched customer funds. KPMG's finding is that overall, a robust resolution process appears to have been in place for each product type that is posted into this account and branch affecting discrepancies should not be included within this account, which is a holding account for customer's money. However, KPMG has identified two exceptions – both of which are caused by Postmaster error or failing to follow prescribed process:

    i. Where Postmasters have accepted cheques made out to Post Office as payment for certain services but have **incorrectly** recorded this transaction as having been paid for

Confidential

POL00423571

in cash **and** the supporting information (which would include branch details) **also** then becomes separated from the associated cheque when the Postmaster sends the cheque to the Post Office Cheques Team to process.

ii. When, between November 2015 and April 2019, Postmasters **failed** to follow the then prescribed two part cancellation process for MoneyGram Transactions, which also coincided with unrelated connectivity issues.

6. KPMG has advised that further investigation into these two potential issues is difficult given the lack of available data held within Post Office and is unlikely to add any further information especially in relation to quantification to that already included in their report and this paper. Further, if a branch were to have made such errors, they would manifest themselves as shortfalls which if they dispute, the Historical Shortfall Scheme provides a mechanism for such claims to be investigated.

7. HSF and Peters and Peters have however been asked [This will be done once the report has been finalised and ahead of the RCC meeting] to advise whether these findings and the KPMG report are disclosable as part of Post office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical practices, in both a civil and criminal context.

Questions addressed

What was the scope of KPMG's review, its limitations and findings?

Report

1. KPMG were instructed to perform a review into Post Office's historical operation of suspense accounts. The scope of this review was as follows:

- Conduct research into historical suspense account operating practices pre-March 2019, holding discussions with key individuals and reviewing relevant documentation (where still available) to:
  - i. Identify any additional relevant suspense accounts to the 4 which were identified during their review of Post Office's current operation of suspense accounts.
  - ii. Identify any changes in the suspense account operating processes during the relevant time period, which would significantly alter the way the identified accounts operated and whether these changes could have potentially had an adverse impact on the Postmasters; and
  - iii. Understand whether the historical resolution processes adopted by Post office for dealing with amounts posted into these suspense accounts were sufficient to identify potential instances where amounts should have been reconciled against branch discrepancies made good by Postmaster.
- Undertake historical analysis of balances held within the relevant suspense accounts for the relevant time period (where data was still available) to establish whether postings to these accounts have altered, and if so the potential impact.
- Perform a high level review of the Tier 2 investigation data arising over the past 12 months to inform their understanding of how amounts could get posted to the relevant suspense accounts

POL00423571

KPMG's Findings

2. KPMG's review into how Post Office currently operates the relevant[1] suspense accounts concluded that, given the robust and transparent investigations process that is undertaken, these suspense accounts should not result in Post Office pursuing Postmasters for sums it had or could eventually take to profit (nor had any evidence been presented to indicate Post Office had). This was because sums housed in these suspense accounts were either:

   - not taken to a profit and loss account; or
   - relate to unmatched transactions due to customers (not postmasters); or
   - relate to surpluses rather than shortfalls.

3. KPMG's review into the historical practices did not identify any additional relevant suspense accounts to those which formed part of their review of current practices. Further, KPMG were informed by Post Office employees, including the product team leaders responsible for posting amounts to the relevant suspense accounts that no changes had been made in the operating processes since they had been established[2].

4. As such, KPMG's overarching finding from its review into how Post Office currently operates these suspense accounts should therefore also apply to the historical operation of these suspense accounts, though it should be recognised, as you would expect, Post Office's investigation into discrepancies has evolved and improved, with the introduction of the Tier Two Investigation Team.

5. The two relevant suspense accounts identified by KPMG are the Agent Creditor Suspense Account (ACSA) and the Customer Creditor Suspense Account (CCSA). Taking these in turn:

   - The ACSA holds surplus discrepancies which Postmasters (as opposed to Post Office) dispute being due back to them. In respect of this account, KPMG's finding from its review of historical practices is that is has seen no evidence to indicate amounts posted to this account related to shortfalls which should have been repaid to Postmasters.

   - The CCSA should only have items posted to it once it has been determined that they relate to outstanding customer funds (as opposed to Postmaster shortfalls). Thus, branch affecting discrepancies should not be included within this account, which is a holding account for customer's money. KPMG's finding is that overall, a robust resolution process appears to have been in place for each product type that is posted into this account. This process identified instances where amounts needed to be reconciled against branch discrepancies prior to them being posted into this account However, KPMG's has identified two exceptions:

      a. Where Postmasters have accepted cheques made out to Post Office as payment for certain services but have **incorrectly** recorded this transaction as having been

[1] Accounts into which Post Office places sums that could relate to discrepancies at a branch level and from which unmatched sums are taken into the P&L account
[2] It should be noted however that there is no formal documentation detailing what operational processes were or were not in place.

POL00423571

paid for in cash **and** the supporting information (which would include branch details) **also** then becomes separated from the associated cheque when the Postmaster sends the cheque to the Post Office Cheques Team to process ("**Post Office Bulk Cheques Issue**").

b. When, between November 2015 and April 2019, Postmasters **failed** to follow the then prescribed two part cancellation process for MoneyGram Transactions, which also coincided with unrelated connectivity issues ("**MoneyGram Issue**")

Each of these are discussed in further detail below.

6. The CCSA was established in April 2010 and the ACSA was established in January 2012. Prior to the establishment of the ACSA, such surpluses remained on Postmasters personal accounts, which were not released to Post Office's P&L account and remained on that account until claimed by a Postmaster. Prior to establishment of the CCSA, the Client Creditor Suspense Account was used to house unmatched customer monies (as well as unmatched client monies). KPMG performed a high level review of transactions posted to Client Creditor Suspense Account from 2005 (the earliest date for which data is available) to 2020 and held discussions with the relevant Post Office employees who manage this account. Limited documentation is available for the Client Creditor Suspense Account prior to 2018, but no further potential issues to those noted above were identified by KPMG.

The MoneyGram Issue: Postmasters failing to follow the two part cancellation process requirements for MoneyGram Transactions and unrelated connectivity problems

7. In November 2015, Post Office made changes to the how MoneyGram transactions were cancelled on Horizon. Postmasters were required to perform a two part cancellation process whereby the transaction had to be reversed through the Postmasters till (the Horizon EPOS) and also cancelled within the MoneyGram interface (also within the Horizon EPOS).

8. In April 2019 Post Office changed the process so that both elements were linked into a one part cancellation process.

9. KPMG were informed by the Post Office MoneyGram product team that during the same time period, MoneyGram transactions experienced connectivity issues.

10. The changes to the MoneyGram cancellation process resulted in an increased number of errors being made by Postmasters when cancelling MoneyGram transactions. In addition, connectivity issues resulted in an increase in unmatched MoneyGram balances that the MoneyGram product team needed to investigate.

11. Post Office subsequently stood up a team of 8 individuals who undertook a large-scale investigation with MoneyGram to try to resolve these unmatched items and identify customers and Postmasters who may be due money back as a result of these issues. This investigation ran during 2017 and 2018.

POL00423571

12. All MoneyGram transactions are date stamped, with each posting also including the branch FAD code. As such, for each MoneyGram transaction, it was possible to identify the branch where it was performed and when.

13. For each unmatched MoneyGram transaction, the investigation team reviewed whether there was any contemporaneous data from the branches identified to indicate that a MoneyGram transaction had not been cancelled in accordance with the two part process.

14. Where the data showed a MoneyGram transaction had been cancelled on Horizon but had not also been cancelled on the MoneyGram interface, on the date in question, transaction corrections were issued to move the loss to the Postmaster. The transaction correction included enough detail for the Postmaster to correct the original error if the money had not been collected by the recipient.

15. Where the data showed a MoneyGram transaction had not been reversed on Horizon but had been cancelled on the MoneyGram interface on the date in question and where the investigations team could identify the issue related to a branch error a transaction corrections was issued to repay Postmasters.

16. Where the data did not indicate a branch error or indicated a customer loss the unmatched sums were posted to the Customer Creditor Account.

17. Investigations did not include speaking to branches unless Postmasters contacted Post office, regarding MoneyGram related discrepancies.

18. Enquiries have been made with individuals still at Post Office who were part of the 8 person investigation team, including the Team Leader. Although weekly MI was said to be produced, reporting on progress, none has been able to be produced owing to emails not being retained (though they would likely be available via the mimecast archive). It has not been possible therefore to determine to total amount returned to Postmasters.

19. What has been determined is that £615,178 could not be matched and was posted to the CCSA in 2017. This was split across 1,804 branches with 97% having a balance of less than £2,000 and the largest balance being £5,400.

20. Given the level of investigation undertaken by a separate team, the ease with which an affected branch and potential branch shortfall could be identified and the level of exposure at each branch, KPMG's view is that the risk that the £615,178 includes a significant balance relating to Postmasters is low and this balance is more likely to relate to customer losses. However, the lack of available documentation means a residual risk remains.

Bulk Post Office Cheques Issue: Postmasters Incorrectly Processing Cheques as Cash

21. A number of products Post Office offers can be paid for through cheques which are made payable to Post Office (as opposed to the client) For instance DVLA payments, These are known as "Bulk Post Office Cheques". There is a defined process for accepting such cheques

POL00423571

and then sending them to Post Office to process which, if followed correctly, should identify any Postmaster Bulk Post Office cheque processing errors, with a Transaction Correction subsequently issued.

22. However, if a Postmaster accepts a Bulk Post Office Cheque as payment but, in error, records that the transaction was paid for in cash, more cash will be expected in the till than is physically there.

23. If when then sending the Bulk Post Office Cheque to Post Office, the branch information which should accompany the cheque also becomes separated from the cheque – the payment is made to the recipient but as there is no matching transaction on Horizon (i.e. as it was processed as cash) it is difficult for the Cheques Team to identify which branch has made the error and for a Transaction Correction to be issued.

24. If Postmasters realise the error they have made, they are able to contact the Cheques Team to rectify the error. Further, the Cheques Team proactively attempt to identify branches where there are high value (>£500) Bulk Post Office cheques with no supporting branch information, but if the branch is not identified, the cheque value is subsequently posted to the CCSA.

25. c£134k has been posted to the CCSA as a result of Bulk Post Office Cheques Issues since it was established in 2010. Although a proportion of this sum could relate to branch shortfalls caused by Postmaster error, it will also include:

    i. Customer losses: e.g. a Bulk Post Office Cheque is processed but a corresponding bill payment is not made / not made in full (for example, a DVLA transaction is not processed through the till on Horizon or the DVLA interface but the cheque is accepted and sent for processing. The cheque is banked by POL but DVLA will not process the transaction or request payment as it is not on their system

    ii. Matching Errors: e.g. the transaction is recorded correctly but the Bulk Post Office Cheque becomes separated from its supporting information when being sent to Post Office for processing. The customer's payment is correctly made, the Postmaster's till will balance but when the cheque payment comes to be allocated to a client, there is no way of knowing which client should be credited as the cheque is made out to Post Office.

26. KPMG's understanding is that it is not possible to identify what proportion of the £134k is made up from matching errors, customer losses or potential Postmaster losses due to the lack of available supporting information documented on the cheque.

Next Steps

27. KPMG has advised that further investigation into these two potential issues is difficult given the lack of available data held within Post Office and is unlikely to add any further information especially in relation to quantification to that already included in their report. In respect of the MoneyGram Issue, this is because of the time that has passed, personnel which have since left the organisation and lack of documentation which exists / has been

POL00423571

retained / was ever produced. In respect of the Cheques Issue, this is for the reasons set out at paragraph 26.

28. If a branch were to have made such errors, they would manifest themselves as shortfalls which if they dispute, the Historical Shortfall Scheme provides a mechanism for such claims to be investigated.

29. HSF and Peters and Peters have however been asked [redacted]

5

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Duplicate Transaction Corrections issue	**Meeting Date:**	12 November 2020
Author:	Tim Perkins, Head of Security, Safety & Loss Prevention	**Sponsor:**	Al Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to note an incident on 14/10/2020 where 571 cash surplus / shortage duplicate Transaction Corrections were issued to 449 Branches in error along with the steps taken to remediate the issue and avoid a reoccurrence.

6

Executive Summary

On 15/10/2020 it became known that 571 cash surplus / shortage Transaction Corrections (TCs) had been duplicated. This was brought to light by several calls from branches to the Branch Reconciliation Team (BRT) and the National Cash Centre Accounts & Reconciliation Team (NCCART), which led to an investigation. The cause was quickly identified as an individual within BRT who had bypassed the quality control mechanism which is for each batch of TCs to be reviewed and signed off by a manager. In this case, the first issue of the TCs on 12/10/2020 had bypassed the quality control check, but the second time these were issued, the individual followed the correct process.
To remediate this, all 449 branches were immediately sent a memoview (Appendix A) to acknowledge and apologise for the error. A further TC to correct the error was arranged and sent the same day 15/10/2020 to correct the branch accounts.

The incident was reported to the Historical Matters Unit for information.

A Branch Focus article was issued to the entire network along with the incident being included in Amanda Jones' regular communication to branches to remind branches to report anything that looks strange or that they do not understand and to assure them we will listen and investigate. (Appendix B)

The matter is being dealt with under the Conduct Code with the individual concerned, with the first step being a full fact-find.

In parallel, investigations are underway with Accenture to establish whether a failsafe can be introduced to prevent either the QA bypass or duplicate TCs being issued.

Confidential

POL00423571

Questions addressed

1. How did this incident occur?

2. What steps were put in place to remediate the incident?

3. What further steps are being taken to prevent such an incident happening again?

Report

4. An incident occurred where 571 duplicate TCs were issued to 449 branches as a result of an individual failing to follow the quality control process. In bypassing this process, the individual sent the first batch without the prescribed check by a manager within the Branch Reconciliation Team and also failed to check these off as a completed task.
5. The second time the TCs were issued, all relevant checks were made, but these checks are designed to ensure accuracy of the TCs and the associated wording for branches and would not check whether the TCs had already been issued since this should not be possible under the process if followed correctly.
6. The incident came to light due to calls from branches which allowed a speedy investigation and a remediation plan to be put in place.
7. The branches concerned were sent a memoview to explain what had happened and to apologise for the incident. Appendix A
8. Additionally, the Historical Matters Unit were informed due to potential repercussions within the context of GLO.
9. A branch-wide communication was issued on 15/10/2020 to report the incident to all branches to ensure transparency of this issue since there is no fail-safe in place today. This communication also reminded branches to contact the telephone number on TCs if they have any concerns as a reassurance to them, although we know this issue was contained to the 449 branches only.
10. The issue is being dealt with under the Conduct Code for the individual concerned and it is expected the full fact find will identify improvement opportunities which will be implemented over the next weeks and months, along with further supervisory checks.
11. Additionally, Accenture have been engaged to explore a technical fail-safe to either prevent management controls being ignored or over-ridden, or preventing duplicate TCs being issued.
12. These last two points are to be pursued by Alison Bolsover and Colette McAteer who manage the Branch Reconciliation Team and have been added to their Q3 objectives.

Risk Assessment, Mitigations & Legal Implications

13. Post Office is addressing this issue consistently with the duties implied by the GLO Common Issues Judgment into postmaster contracts, through its communications to the affected branches and wider network, and by ensuring that affected postmasters are not held liable for any financial impact the issue may have had to their branch accounts.

14. Changes were made to Post Office processes and controls relating to the management of TCs as part of Network Operation's remediation response to the Common Issues Judgment. The incident outlined in this paper demonstrates the importance of ensuring that those processes and controls are subject to ongoing review, monitoring and assurance.

Confidential

POL00423571

Stakeholder Implications

15. The impacted stakeholders in this issue were Postmasters. The actions taken to communicate and resolve the issue mitigated the impact on Postmasters and, to date, no complaints have been raised about the remediation actions taken by Post Office.

Next Steps & Timelines

16. The two actions in place; 1) the full fact find into the incident as part of the Conduct Code and 2) the investigation into a technical solution via Accenture, to be completed by 30 November. In the event of a technical solution being preferred, this will be established as a Prove plan / short project for consideration by PRB and sponsored by Amanda Jones / Dan Zinner.

Confidential

POL00423571

Appendix 1

From: MemoView <GRO>
Sent: 15 October 2020 13:51
To: PostOfficeAccount.RefDataTeam GRO
Subject: FINAL MBS 273 Duplicate Transaction Corrections

Please see approved memoview for release to selected (449) branches only.

MBS 273 Duplicate Transaction Corrections

For information

We have become aware today that Transaction Corrections issued to your branch for Cash Pouches on 12 October have been duplicated on 14 October. We are sorry for this duplication.

We will be issuing compensating Transaction Corrections today which will appear on Horizon tomorrow for you to accept.

We can only apologise for any inconvenience this has caused to you.

6

Confidential

POL00423571

Appendix 2

Extract from Amanda Jones' email to branches sent 22 October 2020

Duplicate Transaction Corrections
Last week some branches received duplicate Transaction Corrections for Cash surpluses/shortages in error. Thank you to branches who called us to raise this issue. The team identified the problem and a compensating Transaction Correction was issued on Horizon for acceptance on Friday 16 October to correct the situation.

The duplicate Transaction Corrections was a result of human error within the Branch Reconciliation team who issue Transaction Corrections. The controls that prevent this type of error occurring are urgently being reviewed and we'll be making changes to improve the process. Mistakes like this do happen, and we'll be open about them with you.

If you receive a Transaction Correction notice and have a question or are concerned about it, the notice will include a phone number to contact for more information. We've provided a full update in this week's branch focus.

6

Extract from Branch Focus – 22 October 2020

Transaction Corrections - Guidance

This is to notify Postmasters that last week 449 branches were issued duplicate Transaction Corrections for Cash surpluses/shortages in error. This was as a result of human error within the Branch Reconciliation team who issue Transaction Corrections.

As soon as we were aware of this error, we sent a memoview (MBS 273) to the affected branches. This explains that the Transaction Corrections issued on Monday 12 October had been duplicated in error on Wednesday 14 October (appearing on Horizon on Thursday 15 October). A compensating Transaction Correction was issued to appear on Horizon for acceptance on Friday 16 October to correct the situation.

The controls that should prevent this type of error occurring are under urgent review and will be updated and amended where necessary, including retraining. However, if you are ever uncomfortable with a Transaction Correction or the reason for it isn't clear, please do call the telephone number which is always provided on the Transaction Correction narrative to report this so we can investigate and make sure it is correct.

Thank you to those branches who did call us about this error. This enabled us to quickly identify the duplication issue and resolve it for the branches concerned.

Thank you for your support and we apologise for the inconvenienced caused by this issue.

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Financial Reporting Controls Environment	**Meeting Date:**	12 November 2020
Author:	Christine Kirby, Financial Controls Manager & Tom Lee, Financial Controller	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting

The Risk & Compliance Committee ("RCC") is asked to note the update on the Financial Reporting Controls ("FRC") environment, including improvements made since the last report to the Audit, Risk and Compliance Committee ("ARC") in 2019 and details on future focus, for onward submission to the ARC.

Previous Governance Oversight

- Prior year report was presented to ARC for noting on 23 September 2019.

7

Executive Summary

Since the last report to the RCC and ARC, the FRCF has continued to be improved through process reviews and controls testing. This has enabled the FRCF to become more streamlined and risk focused. Looking forward, the aim is for the FRCF to transfer to ServiceNow (or another provider) in order to be more agile, efficient and to create synergies between Central Risk and Financial Controls, as well as allowing PricewaterhouseCoopers LLP ("PwC") to mitigate their threat of self-review, as Post Office Limited ("POL") currently use a PwC off the shelf tool called TrAction which has been in place for 3 years.

The FRC environment has continued to be strengthened through enhancements in the biannual Balance Sheet testing, quarterly Finance Director ("FD") Balance Sheet reviews and Balance Sheet reconciliation review processes. A finance working group has been established, in order to drive improvements and efficiencies, specifically in relation to balance sheet related processes, controls and responsibilities.

Confidential

POL00423571

Questions addressed

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

Report

Past and current status of the FRCF

6. The last report to ARC was in September 2019 at which point there were 500 controls split across 26 processes, which addressed 535 individual risks. See Appendix 2 for more details.

7. Throughout the year the Financial Controls team have performed end to end process reviews across 8 of the highest risk and/or oldest processes, scoping out those which were created/reviewed relatively recently as part of wider projects.

8. This has resulted in streamlining the controls framework. The FRCF now holds 438 controls, split across 26 processes, which address 306 risks.

9. The process reviews enabled risks to be streamlined through removal of bespoke risks and focus on Financial Statement Line Item level risks which are more widely applicable. This ensures that the FRCF is aligned clearly with its purpose of ensuring the Financial Statements are not misstated due to error or fraud.

10. The remaining processes are being reviewed on a rolling basis, prioritising the highest risk processes. Risk assessment is based on materiality, risk of fraud and level of manual intervention, along with any known issues which come to light.

11. Of the 438 controls, 346 controls were issued for self-assessment in September 2020. The remaining controls were either not operated due to frequency (i.e. annual, biannual, quarterly) or were control gaps (a risk has been identified and control has been designed but is not yet in operation). See Appendix 1 for more details.

12. Of the 346 controls issues for self-assessment; 96% were operating effectively (2019: 91%). The remaining 4% includes 1% of controls not self-assessed due to illness and 3% of controls self-assessed but not operating. Reasons for controls not operating include resource issues, delay in meeting deadlines and requests to change control ownership. All controls not operating are followed up and investigated.

POL00423571

13. The results of the Control Self-Assessment ("CSA") are reported to the Chief Financial Officer ("CFO") on a monthly basis, whilst providing an update on the wider FRC environment.

14. In the prior year there were 28 control gaps, as at September 2020 there are 10 control gaps. These are all classed as medium or low risk due to having mitigating controls and/or due to being non–key controls. The remaining gaps are largely due to system limitations and are therefore expected to be long term gaps.

15. Controls testing is performed by the Financial Controls team on an annual basis to ensure each control is tested back to auditable evidence at least once a year. If a control does not meet the expected standard, it is retested again within the year. The controls testing results have improved year on year thanks to the feedback control owners gain through the testing process.

Wider FRC environment

16. Balance Sheet reconciliations for standard risks GLs are submitted to Central Finance on a quarterly basis and high risks GL reconciliations are submitted on a monthly basis. The reduction of standard risk GL reconciliations to quarterly frequency is in part thanks to improved reconciliation quality which has been a focus over the past 18 months.

17. Detailed Balance Sheet testing is performed by Central Finance on a biannual basis on P6 and P11/P12 balances. The GLs in scope for testing are selected based on risk rating. This testing involves agreeing the GL balances back to auditable evidence in order to assess if any adjustments are required.

18. FD Balance Sheet review files are prepared by Central Finance and shared with the respective business units for their review on a monthly basis. FD Balance Sheet review meetings are held on a quarterly basis to enable Central Finance and Commercial Finance teams to place greater scrutiny over the Balance Sheets for each area.

19. A finance working group has been established to drive improvements and efficiencies, specifically in relation to balance sheet related processes, controls and responsibilities. A focus list has been established and work is under way to enact change in a swift and positive manner with stakeholders from across finance fully engaged. Changes include enhancements to underlying chart of accounts, establishing clear roles and responsibilities and improving reporting processes.

20. During the year, the second annual Grant Thornton LLP ("GT") audit over third parties whose data POL rely on for revenue recognition took place. The scope of the audit was data analysis, IT general controls testing and business process controls testing across POL's largest service providers (e.g. Fujitsu Telecoms, BGL, DXC, JP Morgan). No significant auditing findings or recommendations were identified. All minor observations were fed back to the service providers and have been subsequently actioned.

POL00423571

Assurance over the FRCF

21. Since the last internal audit of the FRCF (May 2019), there have been several internal audits which involved substantive testing of controls in the FRCF including; post BOT controls, accounts receivable controls, minimum controls standard (COVID-19 impact), manual postings to revenue. These audits have identified control recommendations for the relevant business units but no items have highlighted material issues within the FRCF.

22. The most recent internal audit, manual postings to revenue, tested controls which had already been tested by the Financial Controls team and found no difference in the results of the testing. This provides assurance over the quality of the Financial Controls team testing.

24. The external audit identified minimal management letter points, none of which concerned the FRCF or other key FRC related processes discussed in this report. The audit findings were principally related to differences of opinion on judgemental areas or the classification of balance sheet items, neither of which are indicators of issues within the FRC environment.

Governance Risk and Compliance tool

25. The FRCF is currently held on a tool called TrAction, administrated by PwC. Due to increased independence rules, PwC are unable to perform non-audit services for audit clients and therefore plan to cease POL's use of TrAction by April 2022 latest.

26. POL have been looking to move to a new Governance Risk and Compliance ("GRC") tool for some time due to the system limitations of TrAction but this had been placed on hold due to budget constraints.

27. The timing of POL's requirement to cease use of TrAction has fallen in line with the Central Risk team's plans to move to ServiceNow for top down risk assessment from January 2021. In order to work towards a POL wide governance framework being on one GRC tool, the FRCF will migrate to ServiceNow as phase 2 of the same project, with the aim of being live in the system by end of March 2021, budget dependent.

28. This move will reduce manual actions (i.e. through approval workflows and automated notifications), enable audit trail for changes and improve management reporting through availability of comparative data. The shared tool will also help create synergies between the FRCF and the top down risk assessment as the self-assessments for the FRCF will roll up into the risks maintained by the Central Risk team.

Next Steps & Timelines

29. As well as acquiring a new GRC tool, the Financial Controls team are performing a FRCF completeness review to ensure all financial reporting risks are mitigated. The review is a lengthy process and is due to be finalised in FY20/21. The team also continue to perform end to end process reviews to ensure that the FRCF remains up to date. The next processes under review are loss prevention, record to report and bank & cash management.

POL00423571

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

31. The third party revenue data audit performed by GT is ideally going to be brought in house for FY20/21. The internal resource will be an Internal Audit Senior Manager (3A) and a Financial Controls specialist (3B), both roles of which are currently out in the market. The roles will focus on performing data analysis, IT controls testing and business process controls testing.

POL00423571

Appendix 1 – September 2020 Control Self-Assessment Reporting

Controls		Control Gaps				Control Owners		Sept 2020 CSA Results (submitted Oct 2020)					
Process	Total controls	Control gaps	H/M/L Impact of GAPS H	M	L	Owner Assigned	No owner assigned	Controls operated effectively	Self-assessment submitted but control not operated	Controls with long-term remediations	Not operated due to agreed frequency	No self assessment submitted	Controls not included due being annual
Accounts Receivable	8	0	0	0	0	8	0	8	0	0	0	0	0
Agent Remuneration	45	1	0	0	1	45	0	41	2	1	0	1	0
Agent Remuneration Calendar	4	0	0	0	0	4	0	3	0	0	0	0	1
Bank & Cash Management	42	1	0	0	1	42	0	32	0	1	8	0	1
Branch Interfaces and Master Data	5	0	0	0	0	5	0	0	0	0	0	0	5
Cash Centre - Finance and Master Data	11	1	0	1	0	11	0	10	0	1	0	0	0
Cash Centre - Supply Chain	22	1	0	1	0	22	0	17	0	1	4	0	0
Control Environment	18	0	0	0	0	18	0	13	1	0	2	0	2
Fixed Assets	20	0	0	0	0	20	0	12	3	0	4	0	1
HMRC Registration Process	6	0	0	0	0	6	0	5	0	0	1	0	0
Integrated Settlement & Billing - Billing	11	1	0	1	0	11	0	5	2	1	3	0	0
Integrated Settlement & Billing - Settlement	5	2	0	1	1	5	0	3	0	2	0	0	0
Loss Prevention	15	0	0	0	0	15	0	13	1	0	0	0	1
Manage open items	4	1	0	0	1	4	0	2	0	1	1	0	0
Master data management	21	0	0	0	0	21	0	17	2	0	1	0	1
Non Standard Operating Model (OSF)	4	0	0	0	0	4	0	3	0	0	1	0	0
Payroll	37	1	0	0	1	37	0	29	0	1	4	0	3
Procure To Pay	25	0	0	0	0	25	0	15	0	0	3	0	7
Profitability (COPA)	7	0	0	0	0	7	0	0	0	0	0	0	7
Project Accounting	10	1	0	1	0	10	0	9	0	1	0	0	0
Record To Report	35	0	0	0	0	35	0	28	1	0	5	0	1
Stock	11	0	0	0	0	11	0	6	0	0	2	2	1
Tax	18	0	0	0	0	18	0	10	0	0	1	0	7
Transaction corrections #1	42	0	0	0	0	42	0	41	0	0	0	0	1
Transaction corrections #2	3	0	0	0	0	3	0	3	0	0	0	0	0
Treasury	9	0	0	0	0	9	0	6	0	0	0	0	3
	438	**10**	**0**	**5**	**5**	**438**	**0**	**331**	**12**	**10**	**40**	**3**	**42**

7

Explanation of key columns:

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

POL00423571

Appendix 2 - June 2019 Control Self-Assessment Reporting

Reported to ARC September 2019

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

7

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	PwC Agreed Upon Procedures	**Meeting Date:**	12 November 2020
Author:	Brian Kelly, Finance Director - Tax, Treasury and Working Capital & Tom Lee, Financial Controller	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to note:

i. the scope, purpose and status of the Agreed Upon Procedure ("AUP") engagements performed by PricewaterhouseCoopers LLP ("PwC")
ii. the findings and recommendations made by PwC
iii. the actions performed by Post Office Limited ("POL") in response to PwC's finding

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

8

Several contractual arrangements which POL have with third parties require POL's external auditors to perform AUP engagements to review specific processes, controls and policies in place at POL with regards to each stakeholders interest. These partners are as follows:

- Department for Business, Energy and Industrial Strategy ("BEIS")
- Bank of England ("BoE")
- Royal Mail ("RM")
- Driver and Vehicle Licensing Agency ("DVLA")

The BEIS and RM reports are being finalised and should be complete by the end of November 2020. No material issues are expected.

The DVLA and BoE reports have been shared with each of the stakeholders. The stakeholders have confirmed that they are comfortable with the findings noted.

The Treasury team have put in place an action plan to deal with the BoE recommendations, most of which have already been completed. The remaining actions will be closed off by the end of November 2020.

Confidential

POL00423571

Questions addressed

1. What is the scope and status of the AUP engagements performed by PwC?

2. What were the findings and recommendations raised by PwC?

3. What actions have been performed by POL in response to the PwC findings?

Report

Overview of AUP engagements performed by PwC

4. BEIS AUP – review the accuracy of the financial covenant calculations which are reported throughout the year to BEIS and compare the reported position, for a sample of months across the financial year, to the management information from which they were obtained.

5. BoE AUP – provide a report on Post Office Limited's processes surrounding the Notes Circulation Scheme (NCS) and on the suitability of design and the operating effectiveness of its controls for the financial year under review.

6. RM AUP – comparison of revenue figures reported weekly to RM back to underlying financial records and cash receipts, for the financial year under review.

7. DVLA AUP – comparison of the annual statement provided to DVLA, showing the volume of DVLA transactions performed in branches, back to underlying financial records.

BEIS AUP

8. PwC performed agreed the financial covenant calculations, produced and reported on a monthly basis, back to the data sources from which the information was obtained. The calculations were reperformed and understanding of compliance procedures surrounding the calculation was obtained. The procedures were designed to ensure that POL has met the requirements around calculations and reporting under the BEIS loan agreement for the financial year under review.

9. The PwC report is yet to be finalised but based on discussions between POL and PwC no significant issues have been identified. The only item to note, which will be included in the PwC report, is that the reports provided to BEIS are based on numbers at a specific point in time and are not retrospectively amended. This has no impact on period 1 to 11 as the report is produced at month end close, with any late adjustments being minor. However, at yearend the final numbers may not be agreed until months after the report is issued which could lead to inconsistencies e.g. for FY19/20 the Annual Report and Accounts ("ARA") is yet to be finalised and therefore the numbers reported to BEIS in April 2020 may vary considerably to what will ultimately appear in the ARA. A reconciliation will be included in the PwC report to reconcile the reported position to the latest draft ARA.

Confidential

POL00423571

10. This is not deemed to be an issue as the adjustments made would not, in the instances identified, cause a breach in the covenants. If a breach was to occur then BEIS would be notified as part of the routine ongoing management interactions.

11. The BEIS AUP report is expected to be signed in November 2020.

BoE AUP

12. The report is produced to provide an understanding and examination of the policies and procedures designed and implemented by Post Office to provide user entities with Note Circulation Scheme services (NCS). It looks at the Suitability of Design and Operating Effectiveness of its Controls for the period from 1 April 2019 to 31 March 2020.

13. Continued membership of the NCS Scheme is dependent on meeting the Bank's reporting requirements as well as its security standards.

14. The Bank of England Rules on the Note Circulation Scheme defines how Note Recirculation Facility (NRF) declarations should be calculated.

15. PwC reported 28 individual findings in their audit of the NCS scheme (see Appendix 1), 12 of which were because of evidence not being available due to COVID-19 restricting access to sites and therefore preventing physical inspection.

16. BoE have reviewed the reported findings and confirmed with POL at the October 2020 Quarterly Compliance call that they have no concerns about the findings due to their immateriality.

17. No material control failures were highlighted, however, management recognise the need to take action to ensure Post Office is fully compliant with the rules of the scheme and maintain a good relationship with the Bank of England. The findings have been summarised at a high level in paragraphs 18 and 19. The detailed list of individual findings can be found in appendix 1.

18. Staff Knowledge, Training and Access:
    - Limited evidence of staff training in the team;
    - A user access list for Team Drive, SharePoint and the NIPS system could not be obtained for the full year;
    - No evidence was provided to demonstrate that a review of the NIPS system user access list was performed in the year;
    - The spreadsheets used to calculate the daily NFR position should all be password protected.

19. Other findings:
    - Signed audit packs and CCTV footage from cash centres which validate key controls have been performed could not be accessed due to restrictions in place for COVID-19.
    - Multiple instances when the Cash Centre Managers did not confirm the daily forecast as per the agreed control

POL00423571

20. Whilst the findings are not material, management recognise the need to address the findings and have agreed the actions in Appendix 2 with the Treasury team. Most of the actions have been completed, with the remaining due to be completed in November 2020. Note the findings will appear in the FY20/21 PwC report, despite being cleared, as they will have been applicable for part of the financial year under review.

RM AUP

21. PwC performed a review of POL's gross actual revenue for the year ending 29 March 2020. This involved casting the 'breakdown schedule', agreeing the schedules to the POL General Ledger and agreed the total gross revenue to the bank statement.

22. One exception was identified where the gross revenue per the GL and per the bank statement was greater than the 'breakdown schedule' by c. £10m. This was an overpayment to Royal Mail which was subsequently returned the following week – management were aware, rectified this at the time and no further instances have occurred as a result of controls in place.

23. As part of POL's requirements to provide all relevant information to PwC which could impact RM revenue, POL also notified PwC of an issue regarding the application of new stamp tariffs which occurred in Feb 2019, resulting in under settlement of c. £500k to RM which was resolved post year end. This was noted in PwC's report but RM were fully aware and subsequent settlement has been performed.

24. POL has also informed PwC about the stamps review (Project Frank) performed in the year by KPMG LLP. PwC are due to sign a hold harmless letter to enable them to review the KPMG report directly to ensure there is no impact on the AUP report or managements associated representation letter. Once this has been closed off the PwC AUP report will be finalised for signing, expected to be November 2020.

DVLA AUP

25. PwC performed walkthroughs of the end to end DVLA transaction process, reconciliation of SAP data to Horizon data, sampling transactions to ensure they flowed through from Horizon to the bank statement, analytical review of sales and remittances and reperformance of key calculations driving the Annual (volumes) Statement provided to DVLA.

26. PwC identified some minor findings in relation to daily reconciliation variances, which were subsequently resolved, and sizable movements in sales balances in branches, which were suitably explained. Additionally, an IT finding was included as a general point around user access controls, which was noted in the main yearend ARA audit and included in this report for completeness as it was in relation to branch system access controls.

27. Any reconciling differences noted were trivial (less than £5k) and 'unusual movements' noted in the analytical reviews have been backed up by management responses.

POL00423571

28. The report has been shared with DVLA and no issues have been raised by management.

Conclusion

29. Whilst PwC identified findings through their AUPs, POL management are comfortable that these are immaterial and the overall outcomes of the AUPs demonstrate a strong control environment across the business processes.

30. Any remaining findings and recommendations will be addressed where required ahead of the FY20/21 AUP reviews.

Next Steps & Timelines

31. BOE - The remaining actions in relation to the BoE NCS AUP will be closed by 27 November 2020.

32. RM - PwC are due to sign the KPMG hold harmless letter so that they can review the Stamps report and ensure that there is no impact prior to releasing the AUP report. Report expected to be signed in November 2020.

33. BEIS – final review and clearances are underway and the report is expected to be signed in November 2020.

34. DVLA – None.

Confidential

POL00423571

Appendix 1 – BoE AUP PwC findings

Control Title	Audit Findings
CO1.1 Applicable process and guidance documentation is maintained and made available to the relevant teams - through the networked 'Team Drive' or held locally at cash centres - involved within the NCS process	Whilst we were able to inspect the SharePoint site, we were unable to inspect or observe evidence of the Team Drive used to share data with the relevant teams for the period 1/4/19 - 23/10/19. As such, it was not possible to test the design and operating effectiveness of the Team Drive element of this control.
CO1.2a - Treasury staff are provided with specific on the job training relevant to their role - supported by the process and guidance documentation. CO 1.2b - Cash Centre staff are trained on an annual basis and evidence of the training is maintained through formal training records for each staff member.	We identified that limited or no evidence of training was retained for staff members, and so it was not possible to test the operating effectiveness of this control.
CO1.3 - Team Drive: 01/04/2019 - 23/10/2019 - access to the area of the Team Drive, which holds the NCS forecast spreadsheet, is restricted to only appropriate members of Treasury. SharePoint: 24/10/2019 - 31/03/2020 - Access to the area of the SharePoint, which holds the NCS forecast spreadsheet, is restricted to only appropriate members of Treasury.	Team Drive: 01/04/2019 - 23/10/2019 Exception noted. An access list could not be obtained for Team Drive users within the year. SharePoint: 24/10/2019 - 31/03/2020 Exception noted. An access list could not be obtained
CO1.4 -Team Drive: 01/04/2019 - 23/10/2019 A formal process is in place to ensure that anyone who requires access to Team Drive, and in particular the area where the NCS spreadsheet is held, is reviewed and approved by the Treasury Manager. SharePoint Drive: 24/10/2019 - 31/03/2020 A formal process is in place to ensure that anyone who requires access to SharePoint, and in particular the area where the NCS spreadsheet is held, is reviewed and approved by the Treasury Manager.	An access list could not be obtained for either the Team Drive or SharePoint users within the year, therefore testing over the operation of the control could not be performed.
CO1.5a - Forms requesting new access to the NIPS system from the Bank of England are signed by two authorised signatories prior to being submitted to the Bank of England.	An access list could not be obtained for March 2020. Therefore, we were unable to confirm the population of new users to the NIPS system during the year and pick a sample to test the operating effectiveness of this control.
CO1.6 - The Treasury team maintain a list of individuals who have access to NIPs which is reviewed on a periodic (six monthly) basis to ensure that access to NIPs remains appropriate.	No evidence was provided to demonstrate that a review of the NIPs user access list was performed in the year.
CO1.7 - A formal process is in place to ensure that anyone who requires access to CWC is reviewed and approved by the appropriate Manager.	An access list could not be obtained for the period 01/04/19 - 03/11/19. Therefore, testing could not be performed for user access requests to CWC in this period. For the period 04/11/19 - 31/03/2020, where an access list could be provided, we were able to test without exceptions.
CO1.8 - A formal process is in place to ensure that any leavers from POL have their access to CWC removed in a timely manner.	An access list could not be obtained for the period 01/04/19 - 03/11/19. Therefore, testing could not be performed for user access requests to CWC in this period. For the period 04/11/19 - 31/03/2020, where an access list could be provided, we were able to test without exceptions.
CO1.9 - For the period 4/06/2019 - 31/03/2020 Formulae within the NCS forecast spreadsheet are password protected from inappropriate change within the excel document.	The NCS spreadsheet was only password protected after 4/06/2019. Hence this control was not in operation prior to 4th June 2019. We further noted that one of the tabs within the NCS forecast spreadsheet was not password protected.
CO1.10 - Access to the password to make changes to formulae within the NCS spreadsheet is restricted.	Evidence could not be provided to validate who had access to the NCS spreadsheet password.
CO1.11 - A masterfile log is maintained to detail any changes that have taken place to the NCS spreadsheet or its formulae. Any changes to the spreadsheet or its formulae would require appropriate review and authorisation by the Treasury Manager.	We noted the existence of a masterfile log to track changes on the NCS spreadsheet. However, the contents within the masterfile log are not locked and there are no tracked changes enabled to verify the validity of approvals recorded within the log. Therefore, it was not possible to test the operating effectiveness of this control.
CO2.1 - Team Drive 01/04/2019 - 23/10/2019 Procedural documentation is in place, and available via Team Drive directories, that details the process(es) to be followed in preparing the NRF declaration. SharePoint: 24/10/2019 - 31/03/2020 Procedural documentation is in place, and available via SharePoint directories, that details the process(es) to be followed in preparing the NRF declaration.	Whilst we were able to inspect the SharePoint site, we were unable to inspect or observe evidence of the Team Drive used to share data with the relevant teams for the period 1/4/19 - 23/10/19. As such, it was not possible to test the design and operating effectiveness of the Team Drive element of this control.
CO2.4 - Treasury Manager(s) perform a daily review of the information contained within the NRF / CCO calculation to ensure that the details entered are complete, accurate and valid based upon the associated evidence. Should any discrepancies be identified by the Treasury Manager, an email is sent and saved requesting the amendment.	Exception noted. The treasury team signoff audit review packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 17 out of the 20 samples selected. The remaining 3 out of 20 samples were electronic sign-offs following the new COVID-19 procedures, which we were able to test without exceptions.

Confidential

POL00423571

CO2.5 - The Treasury team sends out the NCS Forecast spreadsheet, including the NRF/CCO calculation, on a daily basis. Each cash centre manager is included in the e-mail distribution list and they should review the information and challenge if there is found to be a discrepancy.	The control which required Cash Centre Managers to respond to the forecast email with their confirmation of acceptance was implemented on 11/06/2019. Therefore, we were unable to test this control during the period 01/04/19 - 10/06/19. For the period 11/06/19 - 31/03/20, we noted that there were 22 instances when the Cash Centre Managers did not respond with their confirmation of acceptance. For the period 11/06/19 - 31/03/20, we were unable to obtain evidence of the forecast being sent and any subsequent sign-offs for 1 sample.
CO2.6 - Finsbury Dials Treasury Analyst will review on a daily basis the forecast submission values at a detailed level, tracing these back to values and other supporting information provided by the cash centres etc. The Finsbury Dials Treasury Manager is responsible for ensuring that the information is complete in the spreadsheet prior to submission to the Treasury Manager for review.	The treasury team signoff of the daily NRF audit packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 10 out of the 20 samples selected. 9 out of the 20 samples were physical copies that had been scanned for review, which we were able to test without exceptions. 1 out of 20 samples was an electronic sign-off following the new COVID-19 procedures, which we were able to test without exceptions.
CO2.7 - The Treasury Manager will independently review and verify the forecast figures that are provided at 10:30am and 13:15pm by each cash centre to ensure the figures are reasonable and conform to the Bank of England's rules for NCS and NRF. Specifically they check that: • The total NRF figure does not exceed the maximum gilts available; • The balance of NRF cash is consistent with previous experience, or there is a known explanation; and • The amounts are reasonable in view of other known information coming from the business, such as cash required in order to meet winter fuel payments, and specific events such as bank holidays.	The treasury team signoff audit review packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 17 out of the 20 samples selected. The remaining 3 out of 20 samples were electronic sign-offs following the new COVID-19 procedures, which we were able to test without exceptions.
CO3.1 - The NCS forecast spreadsheet has in built checks that provide comparisons between forecast and actuals. The Treasury team will investigate differences of +/- 5% and record these differences in the Forensic Investigated Sheets. The outcome of the comparison and associated actions are recorded in the spreadsheet, with details of the clerk and the manager involved in the review.	Exception noted. The treasury team NRF audit packs which validate that this control was performed are currently stored in Post Office HQ. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 10 out of the 20 samples selected. 9 out of the 20 samples were physical copies that had been scanned for review, which we were able to test without exceptions. 1 out of 20 samples was an electronic sign-off following the new COVID-19 procedures, which we were able to test without exceptions.
CO4.2 - On a monthly basis, a review is done by the Treasury Manager to validate the figures entered by the Treasury Analysts and establish where the cap has been breached. The yearly cap forecast is then updated to reflect the anticipated outflows and, where a breach has occurred, make adjustments to ensure the annual cap is not exceeded.	Exception noted. Due to COVID-19 and office access restrictions we could not obtain physical evidence to validate the operation of this control. Therefore no detailed testing has been performed for this control.
CO5.3 - Bond movements are entered into NIPs by cash-centre cashiers. These are then reviewed and agreed by the Cash Centre Management and Treasury team. Where differences/errors are found, they are investigated and rectified on the NIPS.	Exception noted. The treasury team signoff of the daily NRF audit packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 10 out of the 20 samples selected. 9 out of the 20 samples were physical copies that had been scanned for review, which we were able to test without exceptions. 1 out of 20 samples was an electronic sign-off following the new COVID-19 procedures, which we were able to test without exceptions.
CO5.4 - The Finsbury Dials Treasury team will verify the NIPs Bond movement entries against the Bond movements agreed with cash centres for NCS reporting purpose (i.e. daily NCS forecast spreadsheet).	The treasury team signoff of the daily NRF audit packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for 10 out of the 20 samples selected. 9 out of the 20 samples were physical copies that had been scanned for review, which we were able to test without exceptions. 1 out of 20 samples was an electronic sign-off following the new COVID-19 procedures, which we were able to test without exceptions.
CO7.1 Bond access is limited to the hours of 04:00 to 22:30. The vault door is automatically time locked between the hours of 22:30 and 04:00. Requests to access it outside the opening hours would require an engineer.	Due to COVID-19 related office restrictions, we could not obtain the CCTV footage to validate the operation of this control.
CO7.2 Two separate sets of keys are required to open the vault grille which are stored separately in the Traka system safety lock that is only accessible to 4 individuals via their own biometric and ID details. Each individual has access to only one set of keys. When vault access is not required, the vault is locked and both sets of keys are stored in the Traka system safety lock.	Due to COVID-19 related office restrictions, we could not obtain the CCTV footage to validate the operation of this control.
7.4 Control introduced for extended hours from the 19/12/2019 The treasury team consolidates the Bond movement files submitted from the cash centres and checks the entries against the final NIPS transaction reports and NIPS RTGS2 screen. The consolidated Bond movement file is then submitted to the Bank before 15:00.	Exception noted. The treasury team signoff audit review packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020. Due to COVID-19 access restrictions, the treasury team was not able to provide evidence of review for the period of 19/12/2019 to 16/03/2020 For the period of 17/03/2020 to 31/03/2020, there was limited evidence to demonstrate the treasury team review of the bond movement files and the

POL00423571

	NIPS transaction entries prior to being submitted to the Bank of England. We were therefore unable to validate the operating effectiveness of this control during this period.
CO7.5 - The Treasury team sends out the NCS Forecast spreadsheet, including the NRF/CCO calculation, on a daily basis. Each cash centre manager is included in the e-mail distribution list and they should review the information and challenge if there is found to be a discrepancy. Note that this control is a mirror of control 2.5.	Exceptio ns noted. The control which required Cash Centre Managers to respond to the forecast email with their confirmation of acceptance was implemented on 11 June 2019. Therefore, we were unable to test this control during the period 01/04/19 - 10/06/19. • For the period 11/06/19 - 31/03/20, we noted that there were 22 instances when the Cash Centre Managers did not respond with their confirmation of acceptance. • For the period 11/06/19 - 31/03/20, we were unable to obtain evidence of the forecast being sent and any subsequent sign-offs for 1 sample.
CO7.6 - Finsbury Dials Treasury Analyst will review on a daily basis the forecast submission values at a detailed level, tracing these back to values and other supporting information provided by the cash centres etc. The Finsbury Dials Treasury Manager is responsible for ensuring that the information is complete in the spreadsheet prior to submission to the Treasury Manager for review.	Exception noted. The treasury team signoff of the daily NRF audit packs which validate that this control has been performed were stored in the Post Office HQ for all reviews performed prior to the 17/03/2020.
CO7.7 - The Treasury Manager will independently review and verify the forecast figures that are provided at 10:30am and 13:15pm by each cash centre to ensure the figures are reasonable and conform to the Bank of England's rules for NCS and NRF. Specifically they check that: • The total NRF figure does not exceed the maximum gilts available; • The balance of NRF cash is consistent with previous experience, or there is a known explanation; and • The amounts are reasonable in view of other known information coming from the business, such as cash required in order to meet winter fuel payments, and specific events such as bank holidays.	Exception noted. The treasury team signoff audit review packs which validate that this control has been performed are stored in the Post Office HQ for all reviews performed prior to the 17/03/2020.

Confidential

POL00423571

Appendix 2 - BoE AUP POL action log

Actions:	Owner:	Resolution Date:
New Treasurer appointed to focus on improving controls and process improvements	Brian Kelly	Completed
Implement a new training log that is reviewed and signed off half yearly by all members	Pete Mitchell	27.11.20
Request additional training from the Bank of England	Pete Mitchell	Completed
Maintain an up to date list of current users for the NIPS system	Mark Wood	Ongoing
Add a new control in Traction to complete a monthly review of access rights	Pete Mitchell	13.11.20
Ensure password controls are in place for all spreadsheets used in the preparation of the daily NRF calculation	Andrew Ashall	Completed
All treasury documentation to be moved electronic format where possible	Andrew Ashall/Mark Wood	Completed
Management will remind both Cash Centre and Treasury staff of ensuring email replies are received	Andrew Ashall	Completed
Review usage of Tracka safe lock system reports to provide evidence of dual access controls over the vaults	Andrew Ashall	13.11.20

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Historical Matters – Governance Review	**Meeting Date:**	12 November 2020
Author:	Graham Hemingway, Historical Matters Portfolio Lead and Chris Manamley, HM Finance Director	**Sponsor:**	Declan Salter, GLO Director

Input Sought: Noting & Discussion

The Committee is asked to note and discuss the approached to Governance on Historical Matters (HM) for onward submission to the Audit, Risk & Compliance Committee (RCC).

Executive Summary

HM was set up during September as a ring-fenced Business Unit in order to centralise all the work emerging from the three judgments under a new Director reporting to the Group CEO and Chair; to allow Post Office Executive to concentrate upon current and future business; and to ensure all current procedures are reflective of a new culture that will prevent such Historical events every occurring again.

A revised governance structure has been based upon core elements of the existing Strategic Portfolio Office (SPO) framework with changes to the approval processes. Key elements, as discussed with the CFO and team are:

9

Budgeting and forecasting costs

- These are aligned to the current Post Office Limited (POL) budgeting and forecasting procedures

Financial reporting and accruals

- No Changes made to process used previously
- Reporting improvements made by Finance team

Procurement

- POL procurement processes are used wherever appropriate and Procurement team have supported on legal cost negotiations

Financial communications with UKGI/BEIS–

- HM is to feed information via POL Finance to ensure data consistency and single point of contact

Controls, both financial and over data accuracy

- No changes have been made to control procedures.

Internal audit

POL00423571

- Internal audit have been engaged to carry out reviews of Programme setup/management and the key workstreams delivering into BAU

Risk Management

- Managed via SNOW as per SPO, reviewed regularly by Programme team, reported at SteerCo

Compliance

- Governance – via SteerCo/Decision Forums/Board reporting
- New controls implemented will link to the Controls Framework being implemented by Compliance Director

Risk & Compliance Committee (RCC) and ARC

Two-way link, RCC/ARC highlighting areas which HM addresses addressing and HM Portfolio risks to be flagged to RCC/ARC

Questions addressed

1. What are HM Governance arrangements?

Report

This report covers governance arrangements implemented to support HM under the following themes:

Budgeting and forecasting costs

1. Forecast updated in Anaplan monthly
2. Forecast update communicated to Board
3. HM to be included as part of POL budgeting process

Financial reporting and accruals

4. No changes have been made to processes in use within POL generally
5. Individual projects now set up in SNOW and Anaplan
6. Standard variance reports developed
7. Actual costs and forecasts reviewed by Finance Director
8. Project costs and forecasts reported by project to the Historical Matters Committee
9. HSF and P&P legal costs now analysed at invoice line level and relevant reports produced

Procurement

10. HM follows POL process as its procedures are led by Public Sector buying.
11. HM Finance Director authorises new recruits etc., but not contracts with suppliers
12. Procurement team are involved when new estimates reviewed/rate discount discussions etc. and this collaborative approach saved an estimated £1.5m in August rate negotiations

POL00423571

13. Legal firms, where practical, or where not directed by Board, follow procurement approach (e.g. Scottish legal firms being sought via Crown Services panel) and panel firms used where possible
14. Project Managers undergo training in Procurement processes

Financial communications with UKGI/BEIS

15. HM to feed information to POL Finance to ensure data consistency

Controls, both financial and over data accuracy

16. No changes have been made to control procedures
17. Finance resource has been boosted through the recruitment of a Finance Director and a Programme Accountant

Internal audit

18. Internal audit have been engaged to carry out reviews of:
    a. Programme setup/management etc. – this is to report during
    b. Common Issues judgment – embedding of Operational changes implemented
    c. Horizon Issues judgment – review of gaps etc., following initial gap analysis

Risk Management

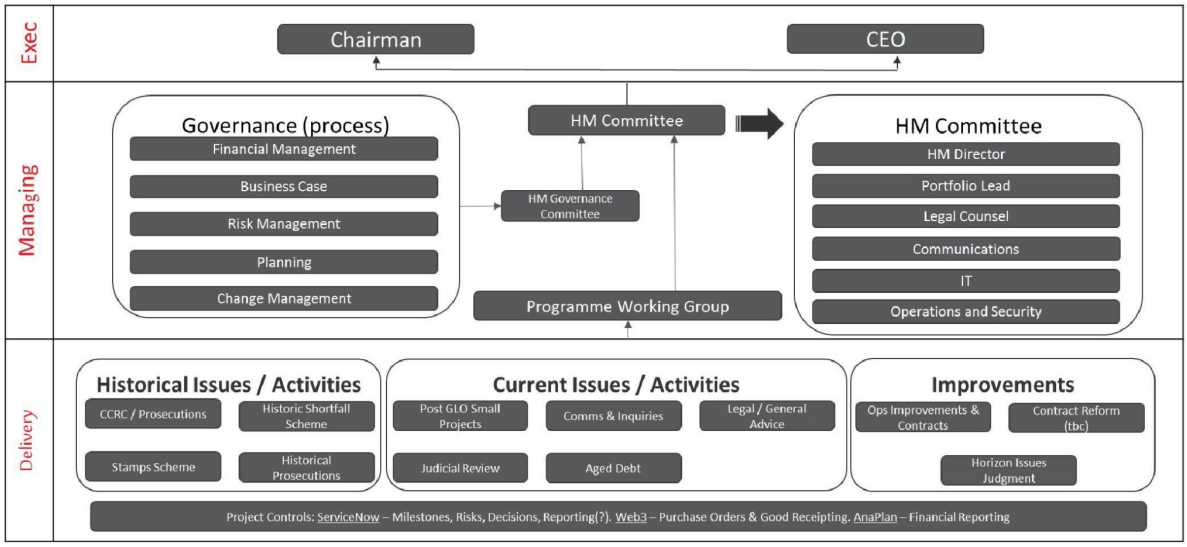
19. Managed via SNOW as per SPO, reviewed regularly by Programme team, reported at SteerCo
20. Portfolio level risks to be reported at RCC/ARC as appropriate

Compliance

21. Governance – via SteerCo/Decision Forums/Board as per diagram below:
    a. Delivery: represents each of the current projects which are enabled to deliver:
        i. Historical Issues / Activities: delivering outcomes to postmasters in respect of past prosecutions and shortfalls
        ii. Current Issues / Activities: ongoing activities such as Legal Advice, Judicial Review, Communications
        iii. Improvements: projects delivering change to operational processes & policy to benefit current postmaster
    b. Managing: represents the functions of the management layer:
        i. Governance / process: the core programme controls in place to monitor and ensure successful outcomes
        ii. Programme Working Group: full programme team and supporting SME working group
        iii. HMU Governance Committee: to review and approve new scope, plans and business cases
        iv. HMU Committee: overarching governance forum accountable for ensuring success of the portfolio delivery
    c. Exec: represents the functions of the management layer:
        i. Board and Senior Stakeholder engagement

Confidential

POL00423571



22. HM is aligned with SPO for the majority of areas, but has separate governance to minimise impact on POL areas – see below table for comparison of SPO and HM approaches (areas in red indicate where HM varies from SPO approach)

CEF / SPO Framework & Controls	SPO	Historical Matters
1 Project Controls		
1.1 Milestone Planning	ServiceNow	ServiceNow
1.2 RAID Management		
1.3 Status Reporting		
1.4 Financial Reporting	ServiceNow / Anaplan	ServiceNow / Anaplan
2 Project Governance		
2.1 Prove Plan: Project set up / budget approval	PRB / IC / Board	Historical Matters Governance Committee
2.2 Business Case: Business case / budget approval		
2.3 Change Management: Milestone / Scope / Budget approval		Programme Change Group / Historical Matters Governance Committee
3 Assurance		
3.1 IT	IT Concurrence / Impact Assessment / HL Design	IT Concurrence at Prove. IT Concurrence at Business Case if applicable including Impact Assessment and HL Design
3.2 Business	Business Readiness Assurance	Business Readiness Assurance, if applicable
3.3 Finance	Finance Director / Technical Finance	HMU Finance Director, Technical Finance
3.4 Portfolio	Head of Portfolio	Portfolio Lead
HM / SPO alignment		HM Finance Director reporting costs, forecast & budget requirements for Programme Spend to SPO via Anaplan
HM / BAU alignment		Historical Matters Governance Committee membership to include POL Head of Corporate Risk aligning HMU with RCC / ARC
HM Change (Scope, Cost, Time)		Historical Matters Exec to brief the Board monthly via standard Board updates. For Change process, see next slide.

23. Work being implemented will also link to the Controls Framework being implemented by Compliance Director, ensuring appropriate controls are delivered – esp. relating to work implemented as part of Common Issues Judgment/Horizon Issues Judgment

Confidential

POL00423571

RCC and ARC

24. As risks are highlighted at RCC/ARC which need HM support to mitigate/treat, they are to be highlighted via Legal & Operations areas (e.g. Data stores, Lottery tickets etc.)
25. In addition, POL Head of Risk is a member of HM Governance Forum to ensure consistency & share knowledge of new initiatives etc. and obtain initial sight of risk areas.

Next Steps & Timelines

The key next steps on these matters include:

26. **RCC/ARC reporting:** Formal links to be established and reporting approach to be agreed
27. **Portfolio Risk Management:** Escalation/tolerances to be agreed for Risks to be highlighted at RCC/ARC

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Financial Conduct Authority pricing rules changes	**Meeting Date:**	12 November 2020
Author:	Ed Dutton, Post Office Insurance Managing Director	**Sponsor:**	Owen Woodley, Chief Commercial Officer

Input Sought: Noting

The Committee is asked to note that:

- the Financial Conduct Authority (FCA) recently announced proposals to prohibit 'Price Walking' (competitive new business prices followed by renewal prices increasing during contract) in Motor and Home Insurance, along with changes to Product Governance and reporting of value metrics; and
- the insurance team have begun to mobilise a programme, overseen by a Post Office Insurance (POI) Board committee, to respond effectively,

for onward submissions to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

- POI Board discussions

Report

Background

1. The FCA have produced their Final Report on General Insurance Pricing Practices 18/1.3
2. They have been reviewing pricing differentials within household and motor insurance for some time. Predominantly, their review work has focused on differentials between new and existing customers.
3. Over time, customers who stick with their insurer can see their premiums increase significantly compared to customers who shop around. This practice is known as price walking.
4. Their work within this area is aligned to a wider Competition and Markets Authority (CMA) review which focuses on pricing in several market areas including general insurance and broadband.
5. The FCA had already concluded that there is significant detriment within the market, highlighting that overall, six million customers were being overcharged for their motor and household insurance, with this overcharging totalling some £1.2bn.
6. There is some evidence that the impact of price walking is felt disproportionally by vulnerable customers and older customers.

10

The Proposed Remedies

7. The core solution proposed by the FCA is that new and renewing customers should pay the same price. This will not prevent the provision by firms of differing prices to customer where the firm operates via different brands and channels.
8. This will require significant changes to pricing models across the industry.

Confidential

POL00423571

9. There will be anti-avoidance measures in place to prevent firms from avoiding the intent of the rules. These will be developed over the coming months.
10. Additionally, Firms will also need more formal processes for assessing products and the FCA will be implementing piloted proposals on reporting value measures.
11. Note that these additional rules apply across GI and not to just household and motor business.
12. Extensive MI reporting on compliance with the new pricing regime will also be required.
13. The FCA notes it will police markets vigorously and will be looking to implement attestation and other requirements as part of this policing process.
14. Under SMCR, it will require firms to be clear on pricing accountability and to focus on fair value, noting that the Boards of regulated firms should have a clear line of sight on pricing practices.

Timing

15. The FCA is now consulting on these proposals.
16. The deadline for consultations on the paper is **25 January 2021**.
17. The FCA then proposes to produce final rules and guidance in the **second quarter of the 2021 calendar year**, with an expected launch date within 4-6 months of that (although the market is unconvinced that is realistic).

Potential Impact

18. Whilst the basic principles of the change are straightforward, there are a large number of technical uncertainties around interpretation. Indeed, whilst the FCA have attended various forums to explain their thoughts to Industry Bodies, it is apparent that conflicting explanations or guidance on specific technical points have been given.
19. Ultimately, whilst the overall market value may reduce slightly, the basic impact will be that value shifts from renewing policies, where margins will reduce, to new business policies, where margins will be significantly higher than now.
20. As a result, the impact appears likely to differ very significantly depending on the size and scale of existing business.
21. This could be:
    - companies that have very significant back books of business where, if they want to sell new business, their renewal prices will have to fall. Or,
    - where large businesses are very complex – the are market comments regarding how many different sets of prices very large consolidated firms like Aviva have in the market – becoming compliant (in terms of governance, reporting AND pricing) could be very complicated, difficult and expensive.
22. POI has recorded a risk that we respond poorly or too slowly – i.e. our pricing model response is mis-judged and our commercial outcomes compared to the current outlook are degraded, or that we are not ready to fulfil the regulatory requirements in terms of our pricing, our governance or the new reporting.
23. However, having (until recently) shrunk our Motor and Home books over recent years, there is the potential for this to be a material opportunity for POI, assuming we can continue to write significant New Business volumes (at higher prices and positive margins) relative to our current (small) mature book size.

Confidential

POL00423571

Activity underway within POI to achieve compliance

24. Given the technical uncertainties, we are working directly with the ABI and BIBA to gain greater clarity from the FCA, and to influence their responses to the FCA consultation paper.
25. We are also already heavily engaged with our main partners (Ageas for Home Insurance and BGL for Motor Insurance), as we have significant dependencies on each other to operate compliantly in the future and to maximise the opportunity/mitigate any risk.
26. POI board has been very focussed on this change in market practice and is overseeing our response via a Board oversight committee, led by a NED.
27. We are in the process of mobilising a focussed change programme to ensure success.
28. The initial activity underway is to generate a more detailed impact assessment of the rules on a set of workstreams, currently including technical pricing, MI and reporting, underwriting partners, finance, governance.
29. This initial discovery phase will inform a more detailed programme scope, deliverables and plan, and resource requirements.
30. Significant change investment and human resources will be required, and specialist resource may be required for some elements.
31. We are reviewing some initial output of this phase for a couple of workstreams on Friday 13th November with the POI Board Oversight Committee, as well as continuing to inform progress on mobilisation of the programme.
32. The programme will follow POL change procedures, as well as be overseen by the POI board, and we will enter the change governance process imminently.

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Risk & Compliance Committee Terms of Reference	**Meeting Date:**	12th November 2020
Author:	Rebecca Whibley, Senior Assistant Company Secretary	**Sponsor:**	Veronica Branton, Group Company Secretary

Input Sought: Discussion & Decision

The Risk & Compliance Committee (RCC) are asked to review and discuss the draft RCC Terms of Reference, including, particularly, the membership of the RCC in light of the recent organisational design changes and then approve the RCC Terms of Reference, subject to any amendments as agreed by the RCC during its discussions for onward submission to the Group Executive (GE).

Executive Summary

Following the adoption of the new Articles of Association for the Group in April 2020, the Company Secretariat reviewed the Group Governance Framework and redrafted the Matters Reserved to the Board and Committee Terms of Reference for all Group Companies. These revised documents were adopted by the relevant Group Companies between April and June 2020. As a result the RCC Terms of Reference required review to align with these changes. Further, the RCC Terms of Reference have not been reviewed since 2016. It is good governance for all committees at Board and Executive level to have terms of reference and for these to be reviewed annually.

As such, the RCC Terms of Reference have been reviewed to align with the new Governance Framework, current practice and to reflect the agreed Terms of Reference structure for the Group.

Given the recent organisational changes, it is understood that this will affect the membership of the RCC and therefore the RCC is asked to discuss and propose the future membership of the Committee as appropriate. The Committee is then asked to approve the Terms of Reference, subject to any amendments agreed, for onward submission to the GE, who will be asked to review and approved the Terms of Reference at its meeting in December 2020.

Confidential

POL00423571

Post Office Limited
("the Company")
Terms of Reference of Risk and Compliance Committee

The Risk and Compliance Committee (RCC) is a standing committee of the Group Executive (GE). Its authority is subject to the powers and duties of the Company Board, as set out in the Articles of Association and the Framework Document.

A. Purpose

1. The purpose of the RCC is to support the GE in fulfilling their responsibilities in the effective oversight of risk management, internal control and assurance, and compliance in the Group.[1]

B. Duties and Responsibilities

2. The RCC shall **review** and **approve for recommendation** (where applicable) to the Audit, Risk & Compliance Committee all papers and decisions prior to submission to the Audit, Risk and Compliance Committee.[2]

3. The RCC shall also:

Risk Management Framework

i. **Review** the effectiveness of the risk management framework and maintain oversight of the development and implementation of the components of the risk management framework;

ii. **Monitor** ~~Maintain oversight of~~ the current risk exposures of Post Office Group and advise on future risk strategy;

iii. **Review** the identification and effective management of current key risks and identified mitigating actions and regular reviews of emerging risks.;

iv. ~~Consider and~~ **Rreview** areas of risk, which should include~~, but is not limited to, sufficient coverage of~~ enterprise and linked intermediate risks.[3]

~~iii. :~~

[1] The Group is defined as Post Office Limited and its subsidiary undertakings: Post Office Management Services Limited (Post Office Insurance) and Payzone Bill Payments Limited.
[2] See the Board Table of Delegated Authorities for decisions requiring Audit, Risk & Compliance Committee approval.
[3] This includes, but is not limited to, Strategic risks, Governance risks (including those related to the financial services businesses operated by the Group and the Company's joint venture (First Rate Exchange Services Holdings Limited), Operational risks, Legal risks, Health & Safety risks (including pandemics), Financial risks, Commercial risks, People risks, Technology risks, Information risks, Security risks, Change risks, Reputation risks and Marketplace & Brand risks.

POL00423571

Post Office Limited
Terms of Reference of the ~~GE~~RCC

~~iv. strategic risk,~~

~~v. major change initiative risk,~~

~~vi. operational risk,~~

~~vii. financial risk, and~~

~~viii. legal and regulatory risks, and~~

~~ix. reputational risk,~~

~~x. plus more specifically,~~

~~xi. people risk,~~

~~xii. fraud risk,~~

~~xiii. technology risk and cyber security,~~

~~xiv. risk relating to the investment strategy and funding requirements of existing and new pensions schemes, and~~

~~xv.~~v. ~~conduct risks relating to the financial services businesses operated by both Post Office Limited and its subsidiaries and joint ventures.~~

Commented [RW1]: Amendment agreed with Mark Baldock as per GE approved enterprise risks signed off in Feb 2020.

~~xvi. Receive and review risk reports from the following~~
~~Transformation~~
~~i. Information Security~~
~~i. Security~~
~~i. Business Continuity (once formed)~~

v. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual risk ~~management~~ management framework~~plan~~;

vi. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft annual internal audit plan;

vii. **Review** risk reports from subsidiaries, as appropriate;

viii. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee the draft risk section of the Annual Report and Accounts;

Internal controls and assurance

~~vi.~~ix. **Review** the adequacy of the Group~~Company~~'s internal controls and make recommendations for the improvement of the Group~~Company~~'s internal controls, processes and systems (including financial controls);

DRAFT

POL00423571

~~vii.~~x. **Monitor** the implementation of key recommendations and management action plans;

~~viii.~~xi. **Review** and **approve for recommendation** to the Audit, Risk and Compliance Committee Key Group Policies;[4] ~~the adequacy of policy governance and recommend changes;~~

xii. **Review** and **approve** Non-Key Group Policies;[5]

Fraud, Theft and Ethics

~~ix.~~xiii. **Review** with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate;

~~x.~~xiv. **Review** any summary of frauds, thefts and other irregularities of any size;

~~xi.~~xv. **Review** with the internal auditors the results of any review of the compliance with the Group~~Company~~'s codes of ethical conduct and similar policies including whistleblowing;

Compliance

~~xii.~~xvi. **Monitor** compliance with legal and regulatory obligations, including any significant breaches and horizon scanning for changes in the legal and regulatory landscape; and

Other

~~xiii.~~xvii. **Review** and **approve for recommendation** to the Audit, Risk & Compliance Committee the Group Insurance provision (including any renewals).

C. Reporting Responsibilities

4. The RCC shall ensure the timely and appropriate reporting to the GE, the Audit, Risk and Compliance Committee and Board (as requested).

5. The minutes of each RCC meeting shall be noted at the subsequent meeting of the Audit, Risk and Compliance Committee.

[4] Key Group Policies are those that require Board/Committee sign-off due to legal or regulatory obligations. A list of Key Group Policies can be found on the Intranet.
[5] Non-Key Group policies are operational policies that do not require Board/Committee sign off. ~~This includes policies which apply solely to Post Office Limited.~~

DRAFT

POL00423571

Post Office Limited
Terms of Reference of the ~~GE~~RCC

D. Authority

6. The RCC is authorised to seek any information it requires from anyone in the organisation in order to perform its duties including calling anyone to the meeting to be questioned as required.

E. Composition and Governance

Membership

7. The RCC shall consist of:
   i. Group Chief Financial Officer (Chair)
   ii. Group Chief Executive Officer
   iii. Group Chief Commercial Officer
   iv. Group Retail and Franchise Network Director
   v. Group Chief Information Officer
   vi. Group Chief People Officer
   vii. Group Operations and Supply Chain Director
   viii. Group General Counsel

8. In the event the Chair cannot attend a meeting, the Committee may nominate a member present to chair that meeting only.

~~8.~~9. Members of RCC may send a nominee to deputise on their behalf with prior approval of the Chair.

10. The following individuals shall be permanent invitees of the Committee:
   i. Compliance Director;
   ii. Head of Risk;
   iii. Head of Internal Audit; and
   iv. Financial Controller.

10. Permanent invitees may send a nominee to deputise on their behalf with prior approval of the Chair.

Quorum

~~9.~~11. Quorum shall be ~~two~~ three members of RCC.

Committee Secretary

~~10.~~12. The Company Secretary, or his or her nominee, shall act as Secretary to the RCC and shall attend all meetings to keep minutes and record actions.

Frequency

~~11.~~13. The RCC shall meet at least six times a year and as otherwise required. Meetings shall be planned in accordance with key reporting and financial planning dates.

Governance

~~12.~~14. Meetings may be held in person or by telephone or other electronic means, so long as all participants can contribute to the meeting simultaneously.

~~13.~~15. Notice of each meeting shall be given to all those entitled to participate at least three working days before the meeting.

Commented [RW3]: Subject to reorganisation to be confirmed.

Commented [R4]: This aligns with GE.

Commented [R5]: Previously two but three is in line with GE

DRAFT

POL00423571

Post Office Limited
Terms of Reference of the ~~GE~~RCC

~~14.~~16. In exceptional circumstances, written requests for approval by RCC may be circulated by email, if agreed by the Chair ~~Group Chief Financial Officer~~.

Commented [R6]: New, but in line with GE

~~15.~~17. Meetings for the RCC will be convened by the Secretary in consultation with the Chair. The Secretary will be responsible for setting the venue date and time of meetings in conjunction with the Chair. All papers supporting the meeting will be issued in good time, three working days in advance of the meeting date.

~~16.~~18. Minutes of each RCC meeting will be circulated to all members of the RCC.

Commented [R7]: Mins to ARC is included above in Reporting section

~~17.~~19. The attendance of other Group employees for part or the whole of any RCC meeting shall be solely at the discretion of the Chair.

F. Annual Review and Approval

~~18.~~20. The RCC will undertake an annual review of its performance and the Terms of Reference. The outcome of these review will be recommended to the GE for approval (notwithstanding amendments approved by the GE whenever so required).

Approved by:	Date:	Version:	Effective from:
Group Executive	July 2016	1.0	July 2016
Group Executive		2.0	

DRAFT

11

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Multiple partner financial stability update	**Meeting Date:**	12 November 2020
Author:	Karl Oliver, Head of Commercial Partnerships	**Sponsor:**	Amanda Jones, Group Retail and Franchise Network Director

Input Sought: Note

The Committee is asked to note the partner financial stability update for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

ARC papers Sept'19 and Mar'20.

Executive Summary

1. In the ARC meeting Sept'19, we shared a paper outlining how we track the financial stability of our largest partners and followed-up with a contingency plan in ARC March'20 which set out how we would maintain PO services in the event of the closure of a large number of PO's as a result of Partner financial collapse. This paper provides an update on the financial tracking of the partners incorporating the known marketplace impact of covid.

2. Of our 6 major partners, 4 are classed as 'Green' (low risk) using our financial stability measures. We do have concerns around McColls and WHS and both are currently classed as 'Amber' (medium risk).

3. Appendix 2 shows key financial highlights for McColls and WHS. For McColls it highlights slight improvements for cash and debt, with share price decline remaining a concern. For WHSmiths it highlights the forecast loss of £70-75m but currently with good access to cash/credit. Neither status has been adjusted and both will continue to be tracked closely as AMBER.

4. Both businesses have been under considerable cost pressures for some time and the impact of Covid has only served to exacerbate this. Our intention has been to work closely with both McColls and WHS to agree pragmatic ways to help them move to a more sustainable estate/model and therefore maintain PO services for customers.

5. As was highlighted in the report to ARC in September last year, we have limited access to Analyst/Broker insights to understand the underlying financial health of some of our largest partners. At the time we explored subscription to Thomson Reuters platform that provided additional financial KPIs but this was discounted as it added 'data' rather than insight.

6. Our recommendation is that we re-look at options within a budget envelope of no more than £30k. Options to be reviewed to include retaining access to an analyst and utilisation of an 'insight/knowledge marketplace' (e.g. Gerson Lehman Group, GLG model).

12

Confidential

POL00423571

7. Since we last reviewed the financial tracking and operational plans with RCC/ARC the partner planning has informed the 'early days' covid response and worked well to accelerate our set-up. We have taken the improved reporting and prioritisation from the covid planning to strengthen the partner plan>

Questions addressed

8. How do we track the financial stability of our strategic partners?
9. What is the current financial status for each of our strategic partners?
10. What is POL doing to support/mitigate risk with the AMBER Partners?

Report

How do we track the financial stability of our strategic partners?

11. Following engagement with Risk, BEIS and finance the 'financial resilience tracker' was established in P1, 2019 to formally review finances and significant account activity for our 6 largest partners. The financial measures where appropriate mirror those tracked by BEIS and are reviewed by period looking for any indication of distress.

    External distress signals would include profit warnings; cash constrained – low liquidity headroom; prospective covenant breaches; Poor financial ratios particularly gearing, operating margin, ROI/ROA; credit status downgrade; share price underperformance; failed refinancing and/or new management team.

12. We currently track share price and trend, Experian ratings, key ratios (net debt vs EBITDA, total debt vs equity and interest payment cover) and formal announcements from the partner to create a RAG rating for each partner. Tracking of industry media & social feeds and insight gained from relationships is included under internal measures, with any significant events fed back through Retail Director updates. The P6, 2020 financial tracker is included in Appendix 1.

Confidential

POL00423571

What is the current financial status for each of our strategic partners?

13. High level partner tracker (full tracker in appendix 1)

	McColl's	The Co-operative Group	WHSmith	Blakemore (SPAR)	OneStop	Tesco
# post offices within estate	557	235	206	115 (115 Company + 102 Symbols)	157	81
POL income (£ YTD)	£14.6m	£6.3m	£11.9m	£2.9m	£3.9m	£2.7m
POL Income variance YoY at YTD (%)	99%	88%	61%	95%	91%	79%
Share price % change in last 12 months	-45%	-	-49%	-	-	-9%
Comments	Positive trading (exceeding conv. channel through Covid) but with drop in share price and continued rationalisation of estate impacting topline. Disposals will continue through sale and closure programme	Strong topline growth and debt reduction. One off tax hit of c.£40m led to H1 loss: . Underwriting business sale and store investment announced	Status change triggered by impact of Covid on retail & PO trading, reflected in share price drop. Although WHS are well financed the extended impact of Covid will require WHS to utilise new credit agreements	Strong topline performance through Covid. PO performance returned 90%+ quickly.	Under Tesco umbrella - positive Covid impact. Some challenge around smallest stores loss making. Moved larger stores across to Tesco x 10 PO sites following positive results	Strong financial performance and net debt reduction. Share price has remained steady through CEO change and sales of Tesco Asia and Poland
Overall Level of concern	Medium	Low	Medium	Low	Low	Low

14. Tesco/Onestop (status: GREEN)
    - Company annual accounts published July'20 caused no triggers and show strong top-line performance and reducing debt (c.£0.9b reduction)
    - Strong trading has through covid impacted period (+9.2% in 12w to ending 4/10 IGD)
    - Combined Tesco/One Stop Post Office estate size has remained stable over last 12 m
    - PO trading recovered quicker in Onestop (-5% YoY for last 3 months) with Tesco hit by temp closures for 10 x transfers and local store customer shift (Status: GREEN)

15. AF Blakemore (status: Green)
    - Their last accounts covered the period until Apr,19 and caused no financial triggers
    - SPAR UK sales performance forecast +6% YoY for 2020 (IGD 30/10)
    - Blakemore have continued to review their estate, selling small and acquire larger stores with a net +4 POs in the last 12m and have expressed an interest in c.5-10 additional PO sites stores for 2021.
    - Blakemore's PO performance recovered from an initial drop of 23% YoY to trade at 100% YoY for the last 3 months.

16. The Co-operative Group (TCG) (status: GREEN)
    - Interim results covering period to early July'20 were published in Sept with no financial triggers caused
    - Co-op have benefitted from the impact of the covid lockdown with food market share peaking at 7.2%, the highest it has been for c.20 years (Kantar)
    - Coop have committed an investment of £130m in opening 50 stores, giving 15 stores significant extensions, and giving 100 further outlets major makeovers, creating 1,000 jobs before the end of the year (IGD).
    - Co-ops PO estate has remained stable over the last 12 months at 235 stores and have expressed an interest in c.10 additional POs for 2021
    - Coop's PO performance was -31% YoY in April and for P6 was -10% YoY, further recovery is expected as they extend trading positions through improved PPE set-up.

12

Confidential

POL00423571

17. McColls (status: AMBER)
    - McColls published their interim results in July'20, with overall flat trading figures the share price following an initially positive response has dropped 38% in the last 3 months and although debt has reduced by c.£8m it remains high
    - LFL trading was +8.3% (McColls interim results) with trading during covid period +c.20% and c.+4% vs Convenience sector through Mar-May (Neilson)
    - McColls have continued their estate review with a net PO reduction of 5 sites and a further 84 (15 closures and 69 to be sold) will be disposed of as part of this programme
    - McColls PO performance recovered quickly benefitting from local shopping, initial drop in April was -20% YoY and average PO trading for the last 3 months of +3.5% YoY

18. WHS (status: AMBER)
    - WHS published interim results in May'20 and a further trading update in Aug'20 in response to the covid impact on both their high street and travel businesses
    - WHS share price has dropped by 49% following the covid outbreak and they moved quickly raise funds through a share placing and to secure access to enough credit to cover an extended period of limited trading (c.£400m at May 20, WHS accounts)
    - We have 7 x PO resignations from WHS where they have failed to reach agreement on new terms with landlords
    - PO performance has recovered from -63% YoY in April to -25% YoY for the last 3 months but lockdown 2 is likely to negatively impact as WHS sites are 'town centre' sites

What is POL doing to support/mitigate risk with the AMBER Partners?

19. McColls
    - We have maintained our controls and contingency plan for a McColls failure (as covered in Mar'20) but are working closely with them on the rationalisation of their estate as they continue the transition from 'Newsagents' to 'convenience operators'
    - They have shared the detailed store disposal plan and how this impacts the operation of POs in their estate. Their estate review will reduce their PO sites by 134 sites, from 607 to 473 (with c.50 completed so far). This 134 site reduction will be achieved through the closure of 52 sites (37 closed) and sale of 82 sites (13 sold). They are reducing their overall retail estate by c.350 sites over the same period.
    - The remaining 15 sites for closure all have closure dates in this financial year. McColls have served full notice on all sites and have extended past official closure dates to assist when we have temporary operators in place (4 stores re-opened with temporary Postmaster).
    - We have proactively advertised all the 'for sale' sites through our 'Run a Post Office' website to help McColls find buyers, with 13 now sold; 50 are 'under offer' and the final 19 remain advertised.
    - We continue to support McColl's Post Office with operational advice, resource mapping and training of additional support staff for covid impacted stores.

POL00423571

20. WHS

- PO are supporting WHS with resource modelling so that they can adjust their labour cost to meet the 'new' demand levels. To date, we have identified c.4,000 hours (c.19% of total) per week of excess colleague workload that due to drop in demand is no longer required.
- WHS demonstrate maintained PO services across their estate throughout the covid impacted period, even where the retail store wash closed, which has been recognised by the customers, with the primary customer service indicator increasing 19% vs previous year, increasing from 65% to 84%. We will continue to track and work jointly to ensure service standards are maintained through cost reduction activity.
- In the medium term, WHSmith PO remuneration remains c.25% down and the post-lockdown retail forecasts show limited recovery with the shift in customer patterns and behaviour away from larger city centres and shopping centre locations expected to continue.
- WHSmith and POL are jointly reviewing variable trading formats in order to provide optimum service levels and introduce flexibility, addressing WHSmith's concerns around PO operating profit/costs, realigning of their staff costs and maintaining high customer service levels.
- Our field teams have extended the McColls approach, covered in the Mar'20 ARC paper, of building individual branch plans for the WHS estate.

Options under review:

- Reduction of counters enabling downsizing of the PO area to allow increased retail
- Introduction of a Combi counter to allow integration of retail & po operation
- New format propositions being considered by POL for simpler more efficient service
- SSK Automation – colleague capability build to drive migration to SSKs
- Trial of opening hours - reduction in quietest periods, aligning with current DMB hours

12

Confidential

POL00423571

Appendix 1

1. Copy of P6 Financial resilience tracker (page 1 of 2)

Period 06 2020			
Company	McColl's Retail Group PLC	Co-operative Group Limited	WH Smith Plc
Registered Number	00298945	IP00525R	05681969
Commercial Partner	McColls	The Co-operative Group (TCG)	WHS
Listed	YES	NO	YES
Exchange	LSE	-	LSE
Market Cap (£)	26.56M	-	1.31B
Current Share Price (0.00p)	26.00	-	1002
Share price high (L12M) (0.00p)	56.00	-	2660
Share price low (L12M) (0.00p)	14.95	-	584.04
Share price % change (L12M)	-45%	-	-49%
Share price % change (L3M)	-38%	-	-6%
Experian Delphi Score (out of 100)	100	No score	100
Experian Odds of Failure	176:1	No score	176:1
Net Debt/EBITDA	2.5	1.5	-0.1
Net Debt/Equity	3.2	0.9	0.2
Interest cover (Earnings/int.exp)	3.2	0.8	89.5
Financial Year End	27/11	5/1	31/8
Recent Announcements	Interim results July 23, 2019	Interim results September 16, 2020	Interim Results May 14, 2020
Upcoming announcements	Preliminary results expected February 2020	Preliminary results expected March 2021	Preliminary results expected Nov 12, 2020
Notes	Share price dropped 38% after post covid bounce	One off tax changes resulted in H1 loss	Trading update issues 5/8
Finance (RAG)			
Number of Company operated POs within estate	557	235	206
Number of Symbol operated POs within estate	0	0	0
Total of whole estate	c.1400	c.2,500 (food)	c.1,400 (600 High Street; 800 Travel)
Acquisitions Company operated (L12M)	0	2	67
Disposals Company operated (L12M)	53	1	0
Disposals of PO with retail retained CO (L12M)	0	0	0
POL Income (notional) (£) YTD	£14.6m	£6.3m	£11.9m
POL Income variance YoY & YTD (%)	99%	88%	61%
Reported PO P&L (if applicable)	-	-	-
POL Notes:	Positive trading (exceeding conv. channel through covid) but with drop in share price and continued rationalisation of estate impacting topline. Disposals will continue through sale and closure programme: AMBER	Strong topline growth and debt reduction. One off tax hit of c.£40m has H1 as a loss: . Underwriting business sale and store investement announced: GREEN	Status change triggered by impact of covid on retail & po trading, reflected in share price drop. Although WHS are well financed the extended impact of covid will require WHS to utilise new credit agreements: AMBER

12

Confidential

POL00423571

Copy of P6 Financial resilience tracker (page 2 of 2)

Period 06 2020			
Company	A.F. Blakemore & Son Ltd	One Stop Stores Ltd	Tesco PLC
Registered Number	00391135	02462858	00519500
Commercial Partner	Blakemore	One Stop / Tesco	Tesco
Listed	NO	No	YES
Exchange	-	-	LSE
Market Cap (£)	-	-	21.27B
Current Share Price (0.00p)	-	-	218
Share price high (L12M) (0.00p)	-	-	260.4
Share price low (L12M) (0.00p)	-	-	203.7
Share price % change (L12M)	-	-	-9%
Share price % change (L3M)	-	-	-6%
Experian Delphi Score (out of 100)	100	100	100
Experian Odds of Failure	176:1	176:1	176:1
Stock on loan %	0%	0%	0%
Net Debt/EBITDA	0.0	0.0	3.9
Net Debt/Equity	0.0	0.0	1.3
Interest cover (Earnings/int.exp)	0.0	0.0	3.3
Financial Year End	30/4	28/2	28/2
Recent Announcements	Annual accounts published Sept, 2019	Annual Report October 19, 2020	Annual Report July, 2020
Upcoming announcements	Annual Accounts expected Oct, 2020	-	-
Notes	-		
Finance (RAG)			
Number of Company operated POs within estate	115	238 (157 One Stop + 81 Tesco)	
Number of Symbol operated POs within estate	102	0	
Total of whole estate	c.280	c. 900 OS & 8,800 Tesco (WW)	
Acquisitions Company operated (L12M)	8	1	10
Disposals Company operated (L12M)	4	13	0
Disposals of PO with retail retained CO (L12M)	0	0	0
POL Income (notional) (£) YTD	£2.9m	£3.9m	2.7m
POL Income variance YoY & YTD (%)	95%	91%	79%
Reported PO P&L (if applicable)	-	-	-
POL Notes:	Feedback has strong topline performance through covid. PO performance returned 90%+ quickly. Store disposals are 'sold' smaller stores: GREEN	Under Tesco umbrella - positive covid impact. Some challenge around smallest stores loss making. Moved larger stores across to Tesco x 10 PO sites following v.positive results: GREEN	Strong financial performance and net debt reduction. Share reprice has remained steady through CEO change and sales of Tesxo Asia and Poland: GREEN

12

7

Confidential

POL00423571

Appendix 2

Key financials for McColls and WHSmith

McColls

£m	IH20[1]	FY2019	IH19[1]	2018	IH19-IH20 % Change
Revenue	605	1219	611	1242	(1.0)% ↓
Gross Margin	25%	26%	25%	26%	0.0%
Adjusted EBITDA	13	32	13	35	0.6% ↑
EBITDA Margin	2%	3%	2%	3%	0.0%
Profit before Tax	(1)	(99)	0	8	-
Cash flow from Ops	36	20	13	62	177.6% ↑
Free Cash Flow	88	(9)	88	104	0.3%
Cash	71	37	37	29	91.8% ↑
Debt	355[2]	131	127	127	180.5%
Net debt	284[2]	94	90	99	N/A[2]
Leverage (Net debt/ Adj. EBITDA)	21.7x[2]	2.9x	6.9x	2.8x	N/A[2]

- Total revenue decreased by 1.0% to £605m in IH20, primarily reflecting store closures during this period and the temporary withdrawal of scratch cards
  - This was however offset by stronger demand observed in the groceries market driven by the Covid-19 outbreak, particularly for food and alcohol
- There have been a number of factors leading to downward pressures on margin
  - Customers' purchasing behaviours have slightly shifted away from impulse, top-up purchases to planned lower-margin take home products, as well as multi-buys and value items
  - There have also been a number of strategic price investments in some key product areas
  - From an operational perspective, there have been additional costs to put in place health and safety measures for employees and customers
- As a result of adopting the new accounting standard for the six months ended 24 May 2020, the Group's Adjusted EBITDA was £28.0m and Net Debt was £284.3m as at the period end
  - On a consistent, pre IFRS 16 basis however, Adjusted EBITDA for the period was over £13.1m (2019: £13.0m) and Net Debt reduced to £82.0m (2019: £89.7m)

12

Confidential

POL00423571

WHS

Key Financial Highlights - UK

£m	IH20[1]	FY2019	IH19[1]	2018	IH19-IH20 % Change
Total UK Revenue	586	1145	591	1130	(0.8%)
High Street	315	580	331	590	(4.8%) ↓
Travel UK	271	565	260	540	4.2% ↓
Profit before Tax	N/A	157	N/A	152	N/A ↑

Key Financial Highlights - Group

£m	IH20[1]	FY2019	IH19[1]	2018	IH19-IH20 % Change
Revenue	747	1397	695	1262	7.5% ↑
Gross Margin	N/A	60%	N/A	60%	N/A
Adjusted EBITDA	104	200	91	185	14.3% ↑
EBITDA Margin	14%	14%	13%	15%	6.3% ↑
Profit before Tax	N/A	157	N/A	152	N/A
Cash flow from Ops	N/A	149	N/A	143	N/A
Free Cash Flow	1	109	27	96	(96.3%) ↓
Cash	45	49	48	45	(6.3%) ↓
Debt	N/A	229	N/A	47	N/A
Net debt	977	180	221	2	342.1% ↑
Leverage (Net debt/ Adj. EBITDA)	9.4x[2]	0.9x	2.4x	0.0x	N/A[2]

- WHSmith UK's like-for-like revenue decreased by ~1% in IH20 from £591m in IH19[1]
  - The ~580 high street stores saw sales and footfall plummeting, which has prompted the business to review its operational structure and consider cutting up to 1,500 jobs as of August 2020
  - Travel division reported a revenue decline of 73% YoY in July and 84% YoY in June, as the majority of UK airport and rail station stores closed during the first national lockdown
  - The firm expects to report a pre-tax loss of £70-75m for the year ending August 2020
- Group's net debt increased significantly from £221m in IH19 to £977m in IH20[2]
  - On the other hand, the group recently raised £166m from investors to improve the balance sheet, which followed a new lending facility of £120m secured shortly beforehand

12

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Transformation Office Change Update 2020	**Meeting Date:**	12 November 2020
Author:	Saira Burwood, Head of SPO & Joanne Welch, Change Risk & Assurance Manager	**Sponsor:**	Dan Zinner, Group Chief Strategy and Transformation Officer

Input Sought: Noting

The Committee is asked to note an update on improvements implemented to better manage Change, ensure the effective delivery of Change, and to approve further adoption and continued improvement, for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

- ARC update on 13th September 2019
- Risk & Compliance Committee (RCC) update on 7th November 2019
- Internal Audit report dated 4th May 2020

Executive Summary

At the September 2019 ARC meeting, an update was provided on the current short-term focus of the Chief Transformation Officer (CTO) and the centralisation of the Change function. The CTO's plan was focused on immediate improvement in the oversight and delivery of Change ('doing things right') not on the Strategy ('doing the right things'). It concentrated on three areas: People, Process and Perception.

Since then a significant amount of work has taken place and the POL Change organisation has evolved into a centralised, collaborative and effective function with clear accountabilities and management. Capable and competent resources are on appropriately configured teams, the quality of support across Change has increased, oversight has been enhanced through better tooling, new rhythms and reports to provide transparency, and governance processes and controls have been further improved and embedded to drive consistency.

To further support delivery of the CTO plan, a new "Change Control Framework" (CCF) was developed. The CCF was deployed formally to the Change Community and wider Business in February 2020 and has subsequently been captured for onward management within Archer GRC tool. In July 2020, Internal Audit noted that that there was already a noticeable improvement in the consistency and effectiveness of controls operation at programme level. More information on the CCF can be found in the Reading Room.

A continuous improvement programme is in place and opportunities are identified and delivered around our current processes, principles, artefacts, tooling and adoption. Our ongoing learnings from post-implementation reviews, health checks, 1st/2nd line assurance and self-identified gaps and weaknesses through our CCF also continue to drive improvements across Change.

While a lot of progress has been made, there's still more to do. Focus over the last year has been on the Change Community, and further work is now required to bring management along on the overall Change vision and journey. This includes broadening stakeholder understanding of, and conviction for, how 'Change works' at the Post Office to make the process more efficient, and assisting the GE to role model appropriate behaviours of change management, including

Confidential

POL00423571

decisiveness and consequence management while advocating consistency, transparency and following governance rules.

Questions addressed

1. What changes have been implemented across Transformation since the last ARC update?
2. How effective is the CCF in mitigating & managing Change Risks?
3. What lessons have been learnt and what areas will be focused on next?

Report

What changes have been implemented across Transformation since the last ARC update?

1. In September 2019, the CTO set out to embed Change processes and ways of working through consistency, clarification and communication. Initial efforts focused on the Change community and increasing understanding on how to consistently manage and resource a project for delivery, before further engaging the overall business on Change. Three key areas were focussed on (People, Process and Perception) and the following section outlines what has been implemented so far in each of these areas.

2. Regarding the key deliverables relating to **People**, 3 sub-themes were identified:
   a. *Structure Change teams that are fit for purpose and leverage current resources to ensure people are working within their scope and ability*
      i. Project Delivery Team manager in place since November 2019 to directly line manage, develop and track (against performance metrics and project data quality metrics) all Project/Programme Manager (PM), Business Analyst (BA) and Project Management Office (PMO) resources, and ensure appropriate alignment of resources to projects based on their scope and ability, and the project needs.
      ii. Central cross-charging through our ServiceNow tool of BAU resources who work on projects is now in place (e.g. SME, Product Owner, Solution Architect, lawyers) which ensures better forward and historical visibility of all project costs and appropriate accounting. In September, 60 BAU resources were cross-charged.
   b. *Increase the number of capable and affordable Change resources, not necessarily total resources*
      i. We have rebalanced the Change Delivery Skills Group resource split from 47% employees (FTE and FTC) on 31st August 2019 to 53% employees on 31st August 2020 to lower overall costs, with the remainder filled by contractors.
      ii. 100% of Skills Group pool resources undergo an induction, within 1 month of joining Change, on the Change Excellence Framework and the 8 PM minimum standards on which they must comply. We have completed 53 inductions in the last 12 months. A BA framework has also been developed and will be embedded in Q3. Both frameworks include compliance metrics.
   c. *Clearly communicate the value of the centralised Change support team structure and roles and constantly ensure this is fit for purpose and cost*

Confidential

POL00423571

i. The centralised SPO function had 14 FTEs in August 2019 and following the recent restructure in August 2020 now has 9.5 FTEs with an overall cost saving of 30%. While the number of Change projects within has not reduced significantly, efficiencies were made due to better IT tooling, focus on improved data quality and more standardisation across processes. Focus is now on governance, resources, assurance/oversight and further tooling improvements.

ii. Further FTE reductions were made with a 'Portfolio of Change' restructure from 8 portfolios in August 2019, down to 5 portfolios, removing 6 FTEs with an annualised saving of over 40%.

3. Key deliverables relating to **Process:**

a. Operationalise Change routines and rhythms, ensuring consistency and speed across the business

i. ServiceNow has been embedded and adopted and is used as our 'single source of truth' for all project data. It is widely used to produce a variety of dashboards and reports on all aspects of Change delivery including the monthly UKGI Change update report, Portfolio performance metrics, project costs & benefits, Change data quality, resource allocation etc. to drive key decisions by senior management and support PMs in successful project delivery. We have 355 risks and 305 milestones against 92 listed projects today versus 555 risks (included duplications and poor data) and 55 milestones against 132 listed projects in October 2019. (See Appendix 1 – Example of weekly project metrics dashboard)

b. Embed the Governance process and tools, with improved efficiency, effectiveness and agility

i. To reduced administration and increase efficiencies the SPO has agreed and documented a number of exceptional processes for activities which do not suit the standard CEF lifecycle yet still require some light touch governance and oversight (i.e. IT Risk & Resilience, Property CapEx, small BF2 client funded projects, and NDA activities). These are inline with our Change Policy and the CCF to ensure minimum control standards are reflected.

ii. The capture and sharing of project lessons learnt plays a key role in ensuring we learn from our mistakes. The Change community and key stakeholders receive a regular overview of key themes being seen in Post-Implementation Reviews and Project Health Checks (See Appendix 2 – Key PIR Themes Report) and appropriate remediation plans and controls improvements are agreed to further strengthen our overall governance processes and CCF.

iii. The Business Readiness Assurance (BRA) process has been enhanced to ensure earlier stakeholder engagement. New projects attend the Gating forum at project outset to ensure their impacted stakeholders are aware of issues and have been involved in developing mitigation plans. 100% (20) Projects received approval first time in Q2 2020 versus Q2 2019 where 12 projects went through gating with only 25% (3) approved first time and 58% (7) conditionally approved.

Confidential

POL00423571

iv. Following CCF assessemnt, more robust processes and controls have been implemented including reducing spend tolerance (from 10% to 2%) which prevents any project from raising a Purchase Order or committing spend more than 2% above their approved budget.

4. Key deliverables relating to **Perception:**
   a. *Foster understanding, conviction and alignment within the Change community on how the PO "does Change," which includes training and constant "on the job" practice in new ways of working*
      i. More frequent communications are in place to build knowledge and engagement e.g. a weekly newsletter, the All Hands Change monthly meeting, Communities of Practice.
   b. *Bring management along on the overall change vision and journey*
      i. The GE/Investment committee have requested more transparency and a desire to see that we are delivering change consistently and learning from our mistakes, but there is still more work to do here in order to support the GE in role modelling appropriate behaviours of change management including decisiveness and consequence management.

5. This is all underpinned by the CCF which identifies all Change risks, control procedures and remediation. The CCF has promoted a cultural shift, increasing awareness that there are risks to be managed and the importance of adherence to our controls and processes. It has driven accountability across Change with risk and control owners identified, and supported enhanced oversight and assurance of change. Work is now underway to fully operationalise the CCF with periodic assessment on the risks and controls.

How effective is the CCF in mitigating & managing Change Risks?

6. The CCF was developed with support from Internal audit in Q3 2019, deployed to the change community in February 2020 and loaded into the Archer tool in Q2 2020 along with the Change Risks (Enterprise, Intermediate and Local risk register risks). The CCF currently holds 53 controls and includes all the checks, challenges, and reports to enable projects to deliver on time, on budget, to the required quality to enable benefits to be realised. These activities are in place at governance, portfolio and project levels throughout the project life cycle until project benefits are transferred to business areas to track to fruition. (See Appendix 3 for a summary of the CCF)

7. Control procedures have been strengthened by defining the activities undertaken, detailing the type of control, its design, ownership and its frequency of operation. The relationship between each control procedures and the risk it helps to mitigate/manage has been linked within Archer and a standard operating procedure defining how SPO Risks and Controls should be identified, assessed, tested, remediated and reported has been issued.
8. The controls were tested in January and September 2020 with overall control effectiveness levels increasing by 51%. (see Appendix 4, fig.1-4) The testing cycle for each control has

Confidential

POL00423571

been set based on its criticality and frequency of operation. Remediation plans were created where controls were not fully effective. The next scheduled tests are December 2020. All testing has been assured by the Change Risk & Assurance Manager to ensure controls effectiveness levels assigned are valid and control owners have appropriate supporting evidence. A thematic assessment of 1st line Portfolio Assurance has been completed with a formal report produced. This report is included in the reading room.

9. Periodically Change risks residual scores will be re-evaluated based on environmental factors and any improvements made to the control. The overall effectiveness of Risk Controls will be re-assessed by the risk owners as remediation plans complete. Any additional remediations will be captured at this time.

What lessons have been learnt and what will focus be on next?

10. This year 15 PIRs, 6 Project Deep dives and 1 Thematic review has been completed resulting in 50 improvement recommendations. One common theme identified across these reviews has been inaccurate benefits, either due to over estimation, erosion due to changes in schedule or an inaccurate initial cost forecast. These recommendations have resulted in updates to governance forum TORs, benefit & cost forecasting roles and responsibilities and supporting RACI being developed, and additional business training planned for Q3.

11. Business change management practices and suppliers' learnings have also been highlighted and are shared regularly with the wider change community via the PM Communities of Practice. A detailed mapping of recommendations against SPO control area can be seen in Appendix 4 – SPO Controls Assessment fig. 5-8.

12. The lessons learnt repository within ServiceNow has been embedded, with all projects recording lessons throughout their lifecycle. There are currently 157 lessons logged. This repository is searchable and is being used by project managers to identify lessons at project initiation to help them succeed in areas where others have fallen foul.

13. In H2 we plan to focus on the wider business to improve their understanding on how 'Change works' at the Post office and communicate our overall Change vision. This includes senior management and the leadership teams (including the GE) and is particularly important and timely following organisational changes. These session will refresh and reeducate Business Sponsors of Change on our processes, controls and the importance of their role within Change in particular, their accountabilities for benefit realisation throughout a project. This will be supported by a quarterly Change communication to the wider businesses informing them of latest updates and changes.

Next Steps & Timelines

We can return to the ARC in May 2021 to provide an update on the areas of focus identified above if desired.

POL00423571

Appendix 1 – Weekly Project Metric Dashboard

WE 16-10-2020 P7 W3 (Summary - PGS Only) — Printed on: 19/10/2020

Notes:	*All cells are filled with whole numbers	*Includes all Active projects (including NDA) only.	*All numbers are whole numbers representing number of projects in each category
Reporting Period:	P7W3	Date Produced:	19Oct20

All Projects

Portfolio Name	This Week Total	By Metal/Size (P/D Only) P	G	S	Dev Gov	Fund	Stage P	D	Week On Week Total	Clo	New	By Metal/Size (P/D Only) P	G	S	Dev Gov	Fund	Stage P	D	Month On Month Total	Clo	New	By Metal/Size (P/D Only) P	G	S	Dev Gov	Fund	Stage P	D
Banking, Payments & Other	26	1	3	11	9	2	5	21	0	0	0	0	0	0	0	0	0	0	-3	4	1	0	0	0	-3	0	0	-3
Historical Matters BU	14	3	0	11	0	0	12	2	11	0	11	0	0	11	0	0	11	0	11	0	11	0	0	11	0	0	11	0
IT Platform Enablement	25	4	3	9	8	1	11	14	0	0	0	0	0	0	0	0	-1	1	-2	2	0	0	0	-2	0	0	-1	-1
Mails, Travel, FS & Other	25	4	1	17	0	3	11	14	0	0	0	0	0	0	0	0	0	0	-1	2	1	0	0	-1	0	0	1	-2
Organisational Effectiveness	12	1	4	7	0	0	4	8	0	0	0	0	0	0	0	0	0	0	0	1	1	0	-1	1	0	0	-1	1
Postmaster & Network	10	3	4	1	2	0	2	8	0	0	0	0	0	0	0	0	0	0	-1	1	0	0	0	-1	0	0	-1	0
Shared Services	8	1	1	3	2	1	3	5	0	0	0	0	0	0	0	0	0	0	2	0	2	0	0	0	2	0	1	1
Supply Chain	6	1	0	5	0	0	3	3	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	-1	1
Total	126	18	16	64	21	7	51	75	11	0	11	0	0	11	0	0	10	1	6	11	17	0	-1	8	-1	0	9	-3

Risks

Portfolio Name	This Week Total	Status R	A	G	By status E	O	Week on Week Total	Clo	New	Status R	A	G	By status E	O	Month on Month Total	Clo	New	Status R	A	G	By status E	O
Banking, Payments & Other	52	6	33	13	2	50	3	2	5	0	3	0	-1	4	1	9	10	-1	4	-2	-3	4
Historical Matters BU	43	13	26	4	43	0	3	0	3	1	2	0	3	0	3	3	6	4	-2	1	4	-1
IT Platform Enablement	109	25	67	17	88	21	0	2	2	-1	0	1	0	0	14	13	27	2	6	6	10	4
Mails, Travel, FS & Other	67	4	41	22	8	59	2	3	5	-5	2	5	-2	4	13	12	25	-2	7	8	-1	14
Organisational Effectiveness	39	4	27	8	9	30	0	0	0	0	1	-1	0	0	-1	1	0	-3	1	1	-1	0
Postmaster & Network	28	2	15	11	12	16	-3	3	0	0	-3	0	0	-3	-8	14	6	-3	-5	0	-2	-6
Shared Services	8	3	4	1	2	6	-2	2	0	0	-2	0	0	-2	-1	1	0	1	-2	0	0	-1
Supply Chain	20	1	12	7	14	6	5	0	5	0	0	5	4	1	3	6	9	-1	2	2	2	1
Total	366	58	225	83	178	188	8	12	20	-5	3	10	4	4	24	59	83	-3	11	16	9	15

Issues

Portfolio Name	This Week Total	By Rating (Open Items Only) 5	4	3	2	1	By status E	A	Week On Week Total	Clo	New	By Rating (Open Items Only) 5	4	3	2	1	By status E	A	Month On Month Total	Clo	New	By Rating (Open Items Only) 5	4	3	2	1	By status E	A
Banking, Payments & Other	16	0	1	10	4	1	0	16	3	2	5	0	-1	2	2	0	0	3	1	8	9	0	-2	0	3	0	0	1
Historical Matters BU	1	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1
IT Platform Enablement	7	0	1	6	0	0	0	7	-1	1	0	0	0	-1	0	0	0	-1	2	0	2	0	0	2	0	0	0	2
Mails, Travel, FS & Other	4	0	1	2	1	0	0	4	0	0	0	0	0	-1	1	0	0	0	0	1	1	0	-1	0	1	0	0	0
Organisational Effectiveness	9	0	2	3	4	0	0	9	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	-1	0	0	0
Postmaster & Network	7	0	1	3	3	0	0	7	1	0	1	0	0	0	1	0	0	1	2	3	5	0	0	2	0	0	0	2
Shared Services	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Supply Chain	1	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0	0	1	-1	2	1	0	0	-2	1	0	0	-1
Total	45	0	6	25	13	1	0	45	4	3	7	0	-1	0	5	0	0	4	5	15	20	0	-3	4	4	0	0	5

Open Milestones

Portfolio Name	This Week Overdue Total	LO	L1	Next 30d Total	LO	L1	Next 90d Total	LO	L1	Week On Week Overdue Total	LO	L1	Next 30d Total	LO	L1	Next 90d Total	LO	L1	Month On Month Overdue Total	LO	L1	Next 30d Total	LO	L1	Next 90d Total	LO	L1
Banking, Payments & Other	8	0	8	8	1	7	18	2	16	0	-2	2	-3	-2	-1	4	0	4	-15	-4	-11	-1	-2	1	0	-2	2
Historical Matters BU	4	1	3	12	4	8	8	4	4	3	1	2	-2	0	-2	0	-1	1	4	1	3	-4	-2	-2	-3	0	-3
IT Platform Enablement	4	3	1	20	5	15	19	6	13	0	-1	1	3	0	3	1	1	0	-5	-1	-4	2	2	0	0	1	-1
Mails, Travel, FS & Other	3	0	3	14	5	9	8	0	8	-2	-2	0	5	5	0	2	-2	4	-2	0	-2	7	2	5	-5	-2	-3
Organisational Effectiveness	28	8	20	4	3	1	5	3	2	16	4	12	-4	0	-4	-3	0	-3	28	8	20	4	3	1	-4	1	-5
Postmaster & Network	4	0	4	13	0	13	10	0	10	1	0	1	1	0	1	0	0	0	1	0	1	6	-2	8	-8	0	-8
Shared Services	0	0	0	5	3	2	3	2	1	-1	0	-1	4	3	1	1	0	1	0	0	0	3	3	0	0	0	0
Supply Chain	0	0	0	0	0	0	4	0	4	0	0	0	0	0	0	0	0	0	-1	-1	0	0	0	0	4	0	4
Total	51	12	39	76	21	55	75	17	58	17	0	17	4	6	-2	5	-2	7	10	3	7	17	4	13	-16	-2	-14

Weekly report

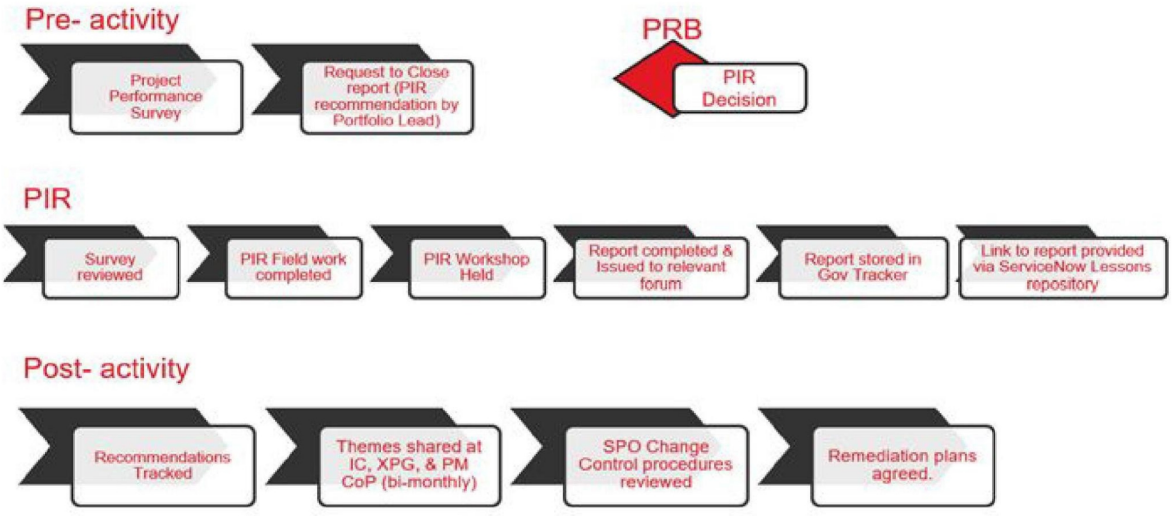
Confidential

POL00423571

Appendix 2 – Key PIR Themes Report (Sept 2020)

Area	Common Findings	Remediation's planned.
Benefits	Benefits can be eroded if Opex costs for supporting processes are not evaluated fully (fraud protection processes) (**E-Pay**), Inaccurate benefit classification and forecasts can lead to decisions being made on incorrect evidence (**Cheque Imaging**). Benefits reduction due to incorrect forecasting and lack of detailed thinking on future cost (**BOT**)or Benefits were not tracked or realised as business cases morph over time (**HIH**)	1. Roles & Responsibilities of Financial forecasting have been reviewed with all key roles, made clearer and are in the process of being deployed. 2. Project closures or formal updates must be provided prior to a new business case being approved to ensure benefits are still valid. 3. Portfolio Leads to request 2nd Line Project health review to help inform senior management if a project should continue.
Supplier Capabilities	Where supplier capabilities are not confirmed with appropriate due diligence, delays and non-delivery can occur (**BOT- Transtrack).** The suppliers initial team lacked experience in Agile delivery leading to a delay in the project achieving required velocity rates. (**HIH- Fujitsu**). Working with a supplier who is also a Business Partner where capabilities are questionable can cause added complexities (**Cheque Imaging- Barclays**).	1. Technical assessments for IT suppliers are to be performed including references. 2. Contractual structure to be more rigorous where appropriate.
Business Change Management	Business Change Management and Business Sponsorship/Ownership is fundamental in large Transformation projects without there will be significant delays and costs will spiral (**BOT**) and business efficiencies will not be achieved. Team engagement needs to be early to take them on the change journey to ensure they have confidence and feel supported at go-live (**E-Pay, Cheque Imaging**). Training, support materials and training systems will be received by end users better where both knowledge and data held reflects real life (**BOT**).	1. Challenges at PRB & IC has been strengthened. 2. Roles and responsibilities of Sponsors and Business Stakeholders to be reinforced. 3. Business Change Management methodology to strengthen CEX and ensure consistent approach is to be developed.
Knowledge Management	Corporate management of legacy knowledge of process and systems was poor, making understanding of the "As Is" virtually impossible, this resulted in rework where both systems and processes needed adjusting at late notice (**BOT**).	1. Project closure activities ensure the capturing and handover of key Corporate Knowledge to ensure on-going management
Product strategy & Strategic direction	Products were being implemented without a clear product strategy which lacked product marketing so customers unaware of new lines (**E-PAY**). A Technical solution was being implemented where a clear business strategy with supporting cost model and roadmap had not been developed which led to frequent changes in direction/scope. (**HIH**).	1. Better processes and ownership in regards to strategy definition & implementation. New organisation structure and roles have been announced.
Resourcing	For large Transformational programmes resourcing must be considered carefully to ensure Business SMEs are available and backfilled where appropriate and specialist roles are brought in house in a timely manner (**BOT**). Initially the resource model was very expensive and agile delivery experience lacking leading to delays and increased costs. (**HIH**).	1. Structure of projects and resourcing requirements are now rigorously challenged by Portfolio Leads and Shills groups line management.

Post Implementation Review Process



13

Confidential

POL00423571

Appendix 3 – The 4 Elements of the SPO Change Control Framework



13

Confidential

POL00423571

Appendix 4 – SPO Controls Assessment (Sept 2020)

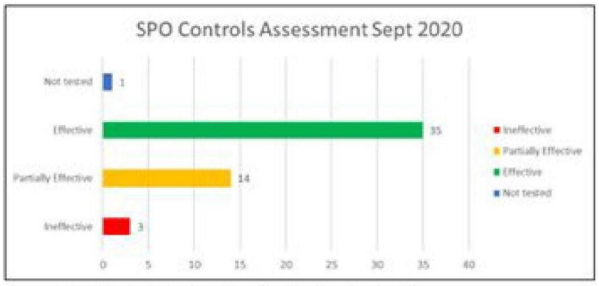


Figure 1. SPO Controls by Test Results (September 2020)

Total Number of SPO Controls is currently 53. Since January 20 new controls have been defined. 27 controls have now tested as effective. 1 test is outstanding while the method to test is confirmed.
Overall effectiveness levels have increased by 51%.

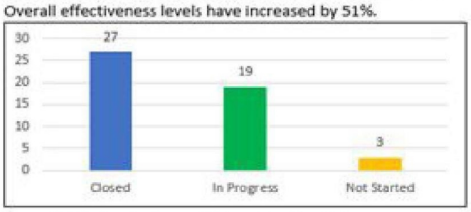


Figure 2. SPO Control remediation plans by status.

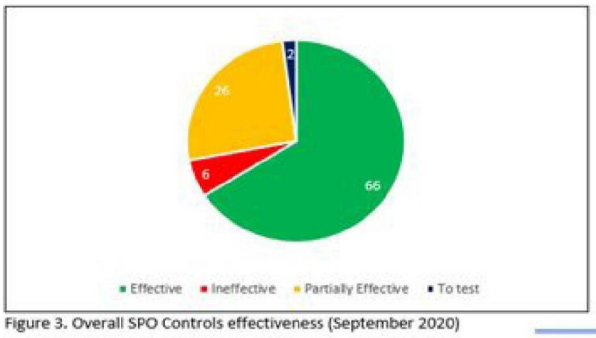


Figure 3. Overall SPO Controls effectiveness (September 2020)

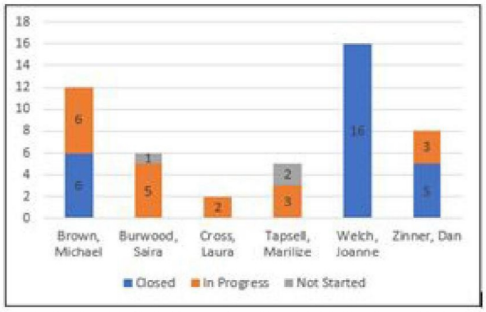


Figure 4. SPO Controls remediation Plan by Person (grouped by status)

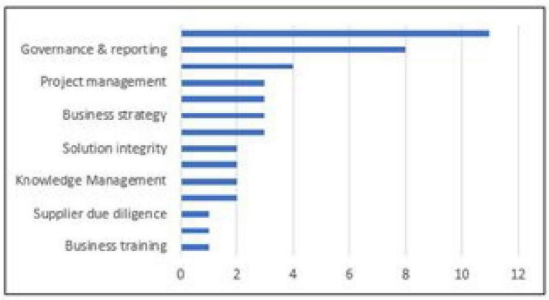


Figure 5. PIR Recommendations by Theme



Figure 6. PIR Recommendations by Impact area

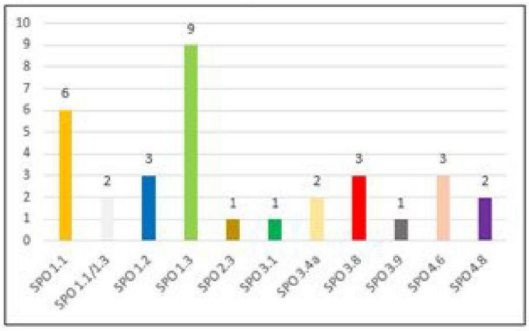


Figure 7. Recommendation Mapped to SPO Control Area

Control Title	Key	SPO Control	Count
Forum TORs		SPO 1.1	6
Roles & Responsibilities		SPO 1.1	2
CEF		SPO 1.2	3
Roles & Responsibilities		SPO 1.3	9
Forecasting R&R		SPO 2.3	1
Finance approval BC		SPO 3.1	1
PRB management		SPO 3.4a	2
Change Requests		SPO 3.8	3
Tranche Funding		SPO 3.9	1
Request to close		SPO 4.6	3
PIR		SPO 4.8	2

Figure 8. Data table to support Recommendation s Mapping

13

Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Payzone Bill Payments Limited Risk Update Report	**Meeting Date:**	12th November 2020
Author:	Michelle Embrey, Quality & Risk Manager & Neil Davey, Operations Director	**Sponsor:**	Andrew Goddard, Payzone Bill Payments Managing Director

Input Sought: Noting

The Committee is asked to note the update on the previous Payzone Risk report last presented to the Risk & Compliance Committee (RCC) and Audit, Risk & Compliance Committee (ARC) in January 2020, for onward submission to the ARC.

Previous Governance Oversight

This is an action from the previous ARC meeting.

Executive Summary

In the January 2020 risk report, Payzone presented 5 significant risks. 4 of these risks had a risk score of 12 and above, with the remaining risk of Brexit being an unpredictable event, qualifying as a 'Black Swan' through its potential to become significant.

Since January, we mitigated the 3 most significant risks of Terminal Communication Issues, GDPR Requirements and Policies & Operating Standards, and also improved and matured the management of the risk framework across the operation of the business.

As a consequence of the Covid-19 pandemic, 4 new significant risks have been determined; the commercial impact on Payzone's clients, poor trading conditions, the dependency on 3rd Parties, and the impact on retailer credit performance. We have been able to limit these new risks to a score of 12 respectively, via a series of management controls and reporting.

The remaining risk from January is the ability for Payzone to deliver forecast revenues vs its original plan. Given the impacts of the recent pandemic this risk has increased from a score of 15 to 20 to become our number 1 risk.

This paper details what steps Payzone has taken to improve managing risk and the movements in our significant risks.

14

Confidentiality

POL00423571

Questions addressed

1. What is the status of Payzone's risk framework and what are the current key risks?
2. What is the approach to risk appetite and key risk indicators?

Report

1. Throughout 2020, Payzone has invested time and resources on its people, teams, and processes to improve the way it manages risk and improves the risk culture:
    a. **Risk Review Meetings**: A risk pack is generated monthly and submitted to Payzone's senior management team for review and discussed during the monthly risk review meetings. The risk owners are challenged on the appropriate mitigating actions that are being taken to ensure the suitability to achieve the target risk scores.
    b. **Risk Structure**: A risk structure has been implemented which has identified the main risk within Payzone (ability for Payzone to deliver the 5-year plan) and promoted to an intermediate risk within the Post Office's Archer risk management system. A diagram has been included in Appendix 1 to illustrate the structure.
    c. **Risk Awareness:** Risk awareness and the role of the risk team has been presented to the wider Payzone business via a business update. There has been separate participation in the weekly team meetings in Retail, Operation and Commercial so individuals can assess and take responsibilities in identifying and mitigating risks in their jobs and teams.
    d. **Rapid Response Team:** Payzone set up a rapid response team through the initial stage of the Covid 19 pandemic and we also participated as part of the Post Office Rapid response team. We helped mitigate a risk in the Post Office Current Account contact centre and their service levels by setting up a separate virtual contact centre using Post Office employees self-isolating.
    e. **Process Improvements:** In 2020, Payzone have matured in continually improving processes to offset risk, with examples in sections 3 and 4 of this paper. Payzone have also set up their own Change Approval Board and Project Review Board. The Change Board has a various number of pre-checks and conversations with key stakeholders to identify risks prior to a change being presented to the Board for approval. Any risks to the delivery of business change and projects are covered in subsequent Change Approval and Project Review Boards.
    f. **Post Office Risk Reporting**: On a monthly basis, an update of the significant risks are reported to Payzone's Risk business partner within the Post Office risk team. This is then consolidated amongst other group risks on the Archer risk management system. This helps us identify if we need any support or resource in managing risk and leveraging if other areas of the business are having similar risks and sharing mitigation practices.
    g. **Alignment on Group Policies:** The Post Office Limited draft policies are now being reviewed by the Payzone Quality and Risk manager, for feedback prior to final submission. This allows Payzone to operate within the policy of the group and understand if any variations to that policy will be required. This has been completed as part of a wider project to adopt or align the policies within Payzone to the Post Office group policies.

    The progress made against the key risks is summarised in Figure 1 with the details outlined in sections 2 & 3 below.

Confidential

POL00423571

Figure 1

Significant Risk	Risk Score	
	Jan-20	Nov-20
Ability for Payzone to deliver forcast revenues	15	20
Poor Trading conditions in current Pandemic	-	12
The impact of the pandemic on clients	-	12
The dependancy on third parties	-	12
The long term impact of the pandemic of finances	-	12
Brexit	5	5
Terminal Communication Issue	20	6
POL Policies and Operating Standards	16	6
GDPR Requirements	16	4

Key Risks

2. January 2020 Mitigated Risks
    a. **Terminal Communication Issue:** In January 2020, the terminal communication issue was the highest risk with a risk score of 20. The mitigations included several IT software releases to improve the communication issue during spring 2020. This has been reflected in a reduction of inbound calls to the Helpdesk regarding terminal communication from 20% down to 4%. Further development has been completed which will enable the ability to complete pre-payment gas transactions on a single device. As a result, the risk score has been reduced to from 20 to 6.
    b. **GDPR Requirements:** Work has been ongoing in conjunction with the Post Office Data Protection team to improve the governance surrounding data protection within Payzone. A data protection process has been implemented which includes data breach reporting and subject access requests. A weekly progress meeting between Post Office data protection and Payzone's Quality and Risk Manager has been set up to provide support and ensure progress of activities. Training material is being created to roll out to all Payzone employees by Q4 2020/21. The actions implemented have reduced the risk score from 16 to a to a target score of a 4.
    c. **POL Policies and Operating Standards:** A project has been set up to align Payzone with the Post Office's key group policies. This proposal was presented to the Sept 2020 PZBP board with the objective to review 2 policies per month until FY Q4. It is the intention that the Post Office key group policies will be adopted where possible. If there are material differences, then variations will be created. The risk score has reduced from 16 to 6.
    d. **Forecast Revenues and Brexit:** These risks remain and are discussed in detail in section 4 of this report.

3. Current Significant Risks
    a. **Intermediate Risk – the ability for Payzone to deliver the 5 yr plan risk score 20 (5:4)**
    This risk has been promoted to become the intermediate risk at group level. The 5-year plan on revenue and cost lines has been re-forecasted as a response to the changing priorities due to the demands on the business from the Covid-19 pandemic. At this stage, we continue to monitor the changes in customer buying behaviour (cash to digital) and the requirements / desire of clients to enter into exclusive contracts as well as plans to migrate to digital payments. To date, we are not seeing evidence of this and in fact, the engagement with clients is more

Confidential

POL00423571

positive and we have advanced dialogue with clients (e.g. e-On, Allpay) and retailers (e.g. Tesco & Coop) to migrate transaction volume to the Post Office and Payzone networks.

b. Poor trading conditions in the current pandemic (risk score 12)

The lockdown in Q1 had a initial downward impact on the bill payment trading conditions with us performing 20% lower against the original budget for the quarter, due to the elderly and high risk shielding at home and our clients working with customers to help them pay their bills through non cash methods or offering free credit and payment holidays. We have seen positive recovery during Q2 with both Energy and Resellers returning to perform -10% against budget and parcels have performed +20% YoY, but transport continues to struggle due to the fear of using public transport and working from home. However, our digital transport solution places in a good position as post-Covid conversion from cash to smart card will be prevalent. We have aided our recovery by signing new Energy clients in Bright and Jersey and driven new volume from eOn, EDF and via our platform partners, Siemens and Itron who prefer to deal with us over competitors. We will drive additional future revenue from a planned exclusive relationship with eOn on smart and from new deals with Allpay and Capita.

c. The impact of the Covid-19 pandemic on clients (risk score 12)

We are starting to see some of the smaller Energy companies struggle and fail due to bad debt and a lack of contingency in their balance sheets. Their customers however are being absorbed by the big 6 suppliers and we have seen 100,000 new customers added to BG's customer base (Robin Hood Energy) which will drive volume to our branch and store network in Q4. The transport industry is in disarray and largely propped up by the government since late spring, which will continue until people can travel freely. Parcel companies are thriving due to an uplift in online shopping and this will continue for the long term, benefitting Payzone via relations with HubBox (start up operator). We are aligned with PUDO strategy work to determine the potential to leverage the Payzone network to support the POL PUDO aspirations.

d. The long-term impact of the pandemic on finances (risk score 12)

The current situation is highly changeable with the unknown impact due to the sporadic shifts in local lockdowns around the country. The actions completed within the credit management function has resulted in a reduction in retailer debt to below the levels seen pre-pandemic. The pre-pandemic levels of failed direct debit were at a level of 1.5% (£182k) per week and a collection rate of 95.5% (£174k). This has reduced to a level of only 0.5% for failed direct debits and a collection rate of 100%. These exceptional levels have been achieved by a combination of activities including improvements to the collection process to collaborate with retailers that fail direct debits, improvements in the quality of new retailers which has been aided with the implementation of a defined credit policy, publicising card payments as well as cash payments. The aged debt levels have also decreased which has been facilitated by a change to how the inbound calls are processed. These calls are now routed to the Helpdesk which has resulted in the credit team's ability to dedicate more time to resolve the older debts.

e. The dependency on third parties (risk score 12)

Confidential

POL00423571

Throughout this pandemic there is a risk to business-critical activities that have a high dependency on third parties which have a possibility for high exposure, for example, PLS which provide Payzone's engineering resource. The key suppliers were contacted and requested to complete a questionnaire to understand their business continuity plan arrangements in place to enable service levels to resume during the pandemic situation. Regular calls are in place with key suppliers to monitor the service during this changeable situation. Additional governance surrounding the control of suppliers is currently being implemented with the development of a procurement policy. The implementation of this policy will ensure the controls in place for external providers are robust and minimises the risk in this area

f. Brexit (Black Swan risk score 5)

The risk to the operation is low based on an appraisal of suppliers and technology processes and the only risk relates to the broader macro-economic impact to the UK economy. This is being continually monitored during the weekly group Covid-19/Brexit rapid response team calls.

Risk Appetite

4. The approach Payzone is adopting to develop the risk appetite is to have the Quality and Risk Manager be a part of the Post Office team reviewing and updating the Post Office Risk Appetite. This will ensure that Payzone aligns where possible to the Post Office Risk Appetite statement. Once the Post Office Risk Appetite has been approved by ARC the risk appetite statements will be reviewed and agreed by Payzone Board during the April meeting.

Conclusion

5. Significant work has been conducted which has achieved a reduction in the overall risk scoring of the pre-pandemic risks. Whilst the COVID 19 pandemic has changed the key risks in the business, the overall risk profile has not changed significantly. Continuous monitoring of how COVID 19 has impacted Bill Payments is in place to ascertain changes to customer behaviour, volume impact, competitor behaviour, and the impact on the operating model.
6. Whilst there has been good progress in the risk framework and maturing the risk culture within Payzone there is still work to be completed to introduce the risk appetite statement. This will be conducted in line with the POL group risk appetite statement. The technology and legal and compliance risk appetite statements are due for approval at the November ARC.

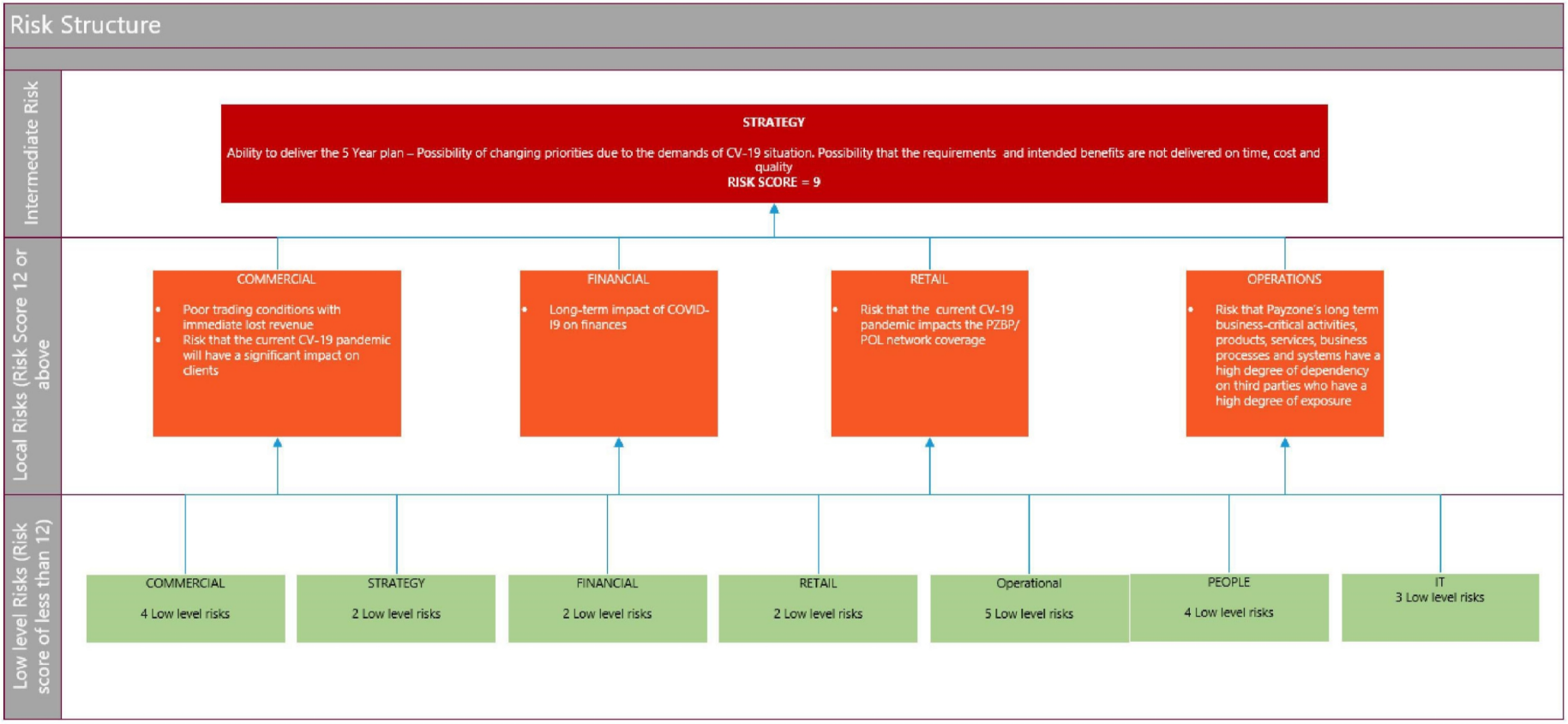
Next Steps & Timelines

7. Risk appetite be generated and brought to the Payzone Board in Q4 '21.

Confidential

POL00423571

Appendix 1: Risk Structure



Confidentiality

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	12 November 2020
Author:	Sarah Gray, Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting

The Committee is asked to note the new or proposed material changes to laws and regulations since the last Risk & Compliance Committee (RCC), for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

There are 4 matters for the Committee to note (details of which are set out in the Appendix):

1. **Restriction of Public Sector Exit Payments Regulations 2020**
   The legislation implementing the £95k cap on exit payments comes into force on 4 November 2020. The cap will apply to any non-exempt termination payments that represent a cost the employer including, redundancy payments, employer pension contributions, and payment in lieu of notice.

2. **Revenue and Customs Brief No.12 - VAT Treatment on Compensation Payments**
   HMRC published its Revenue and Customers Brief 12 (2020) that introduced their new position on VAT treatment of contractual compensation payments. The result of this approach by HMRC will mean that most compensation, early termination and cancellation payments will be considered as payments for supply and will be liable for VAT.

3. **HM Treasury Consultation on new Economic Crime Levy – Update**
   The Economic Crime levy aims to raise approximately £100 million per year from entities regulated for Anti- Money Laundering ('AML') purposes and support reforms to the sustainable resourcing of economic crime.

4. **VAT treatment of Bill Payment products**
   Following a legal challenge from Paypoint, HMRC have changed their view on VAT treatment of Bill Payment products. This change will increase the VAT recovery rate for Post Office and Payzone.

POL00423571

Questions addressed

1. What new or proposed material changes to laws and regulations should the Committee be aware of?
2. What are the implications to the Post Office business?

Report

See Appendix.

POL00423571

Appendix 1

Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
1. Restriction of Public Sector Exit Payments Regulations 2020 ('Regulations')	A cap of £95,000 on exit payments in the public sector has been considered by the Government since 2015. In April 2019, the Government launched a consultation and subsequently published draft regulations. On the 15 October, these Regulations were introduced formally and will apply from the 4 November. They provide that Post Office "must not" pay exit payments (such as that are due upon redundancy) at amounts in excess of £95,000. As such they purport to override employees' existing expectations (some of which are contractual) to redundancy payments.	The Regulations mean that any employees in public sector bodies leaving their business on or after the 4 November will be subject to the £95,000 cap. The Government have not yet published the accompanying guidance to the Regulations, but this is expected imminently. Payments deemed to be exit payments under the Regulations include redundancy payments (with the exception of statutory redundancy payment entitlements), severance payments and contractual payments for lieu of notice. There has been a lot of contest regarding the Regulations, especially from public sector trade unions. The British Medical Association ('BMA') is arguing that the Regulations are unlawful and has asked the courts for permission to apply for a judicial review.	Across the business, 194 colleagues were identified as potentially being entitled to an exit payment above the £95,000 cap. Out of those 194 colleagues, 30 have been further identified as being at risk under the Organisation Effectiveness ('OE') programme. In the event that any of those colleagues were made redundant after 4 November they could suffer reductions under the cap and, if so, could sue Post Office for the capped elements. Those 30 colleagues identified have already been contacted or a conversation has been planned to make them aware of the new Regulations. Any of them that wishes to avoid the cap will also be given opportunity to leave prior to 4 November, as is permissible under Post Office's process. There are also opportunities under the Regulations to apply for exemptions in specific circumstances. Post Office has already submitted a request for an exemption for those affected by the OE programme and will be the first organisation to have done so.	In the short term, whilst initial challenges to the lawfulness of the Regulations are resolved: (i) Post Office will not require employees leaving by way of voluntary redundancy to settle their rights to recover capped elements from Post Office; and (ii) Post Office will apply for exemptions in each case. However, that approach will be kept under review as challenges are resolved and the Government's approach to granting exemptions is better understood.	
2. Revenue and Customs Brief No.12 - VAT Treatment on Compensation Payments	On 2 September, HMRC published its Revenue and Customers Brief 12 (2020) that introduced their new position on VAT treatment of contractual compensation payments. The updated position means that VAT is applicable for:	Until recently, HMRC typically took the view that as compensation or damages payments made under a contract were not consideration for a supply of goods and services, they were therefore outside the scope of VAT. Following two recent EU judgements, HMRC has now reversed this position,	The result of this approach by HMRC will mean that most compensation, early termination and cancellation payments will be considered as payments for supply and will be liable for VAT. This change may also mean significant retrospective impact as HMRC have indicated that anyone who has not	Legal will work with contract owners of key supplier contracts to understand the current contractual position on VAT applicability to these types of payments. Review will also be undertaken into compensation paid under the Group Litigation.	

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-12/11/20

POL00423571

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	(i) Liquidated damages – payments made under contractual obligation to compensate the other party on early termination; and (ii) Payments for breach of contract – contracts which terminate on specific events and provide for a compensatory termination fee. The reasoning provided is that circumstances for terminating are as a result of events envisioned when entering into the contract and are therefore consideration for the supply of goods and services when they occur.	so that many compensation payments or early termination fees will fall within the VAT regime. This change in position was unexpected and industry insiders were given no warning. Many businesses have asked for clarification and further guidance as the cost implication could be huge for companies.	accounted for VAT on the above payments should correct this error. HMRC have provided this should be completed for the usual timescale, which means companies will have to correct any errors over the past four years. This means that Post Office must review whether it has received or made payments for contract termination, liquidated damages and breaches of contract since 2016, and review to understand the VAT position. The legal team have undertaken a review into our standard template contract suite to understand the VAT position on such payments. The review has concluded and advised that no changes need to be made to the template documents as no provision is made for termination payments. Legal are also ensuring that VAT payment for termination fees is taken into consideration when negotiating commercial details of a new contract to ensure this is reflected in the relevant pricing.	Investigation must also occur into whether Post Office have received or made payments that would now sit inside of VAT to understand next steps. Outcomes of the above reviews will be reported in the next Law & Trends Report.	
3. HM Treasury Consultation on new Economic Crime Levy – Update	At the 2020 Budget, the Government announced its intention to introduce an economic crime levy. The levy aims to raise approximately £100 million per year from entities regulated for Anti-Money Laundering ('AML') purposes and support reforms to the sustainable resourcing of economic crime. The proposals included, but not limited to, a levy based on a percentage increase of current AML	Post Office responded to the consultation in October. The expectation is that the official response won't be until 2021, however the draft legislation will likely be published at the same time as the response.	In its response, Post Office were broadly in agreement that a levy based on revenue was the most appropriate mechanism to assess contribution. It raised concerns that if contributions were based on number of SARS this would disincentivise businesses from submitting SARS and this was inconsistent with the AML public policy. Post Office did raise a specific concern regarding calculation of revenue. The calculation of revenue is based only on revenue raised from the regulated activity (in Post Office's case, Travel Money), however Post Office don't earn	Await publication of response to consultation and update accordingly.	

POL00423571

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	fees paid, the size of a business, the number of employees or the number of suspicious activity reports ('SARS') raised.		revenue directly from its regulated activity, it comes from commission paid by First Rate Exchange Services. First Rate Exchange Services are a regulated entity themselves and therefore would also be subject to payment of the levy. This would mean that the levy would be collected twice for one AML regulated activity. Post Office hopes to obtain clarification on this point. Post Office already pay over £2million as a regulated entity and it is anticipated that if we aren't exempt due to the circumstances discussed above, the levy is likely to be either additional tens or hundreds of thousands.		
4. VAT Treatment of Bill Payment Products	HMRC have ruled that the income earned from processing bill payments for clients is now subject to VAT and no longer VAT exempt as it had been treated previously. This rule change has come about following a legal challenge made to HMRC by Paypoint.	Post Office and Payzone ('POL Group') are treated as one VAT Group for HMRC purposes and therefore a joint approach to this change is necessary. HMRC are allowing the POL Group to select a date to enact this change, the sooner the change is enacted the sooner the benefits can be claimed.	The POL Group will benefit financially from this change as it will increase the VAT recovery rate. It is anticipated that this change will deliver an additional c.£1m per year of additional VAT recovery. On top of this recovery, we may also be eligible to submit a historic claim (going back four years) for under-recovered VAT. This would produce a one-off windfall cash refund of c.£4m. The POL Group cannot submit a historic claim until the VAT change has been corrected initially. The circumstances around a historic claim are still in discussion at this point, however we understand than other companies have done so which provides comfort to the POL Group that we would also be able to. A project cross functional group including finance has been set up and there is funding for an initial month and a half of work. The team aims to be able to provide a clearer picture of what it will take to	The project team must continue to investigate the below workstreams: - How do we change business and systems processes; - Impact to our clients; - Legal review of Bill Payments Agreements - Impact to postmasters remuneration; and - Dependency on Payzone (their client list is more substantial that Post Offices and therefore further process change may be required). Deliver a robust plan for implementation and update where necessary.	

Strictly Confidential

POL00423571

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
			deliver this plan by the end of the month. The expectation is that the project will be delivered and completed by the end of the financial year.		

Strictly Confidential

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Data Management in Post Office	**Meeting Date:**	12th November 2020
Author:	Jonathan Hill, Compliance Director Mark Underwood, LCG Operations Director, Laurence O'Neill, Snr Legal Counsel HR & IR Rodric Williams, Head of Legal Dispute Resolution & Brand	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Discussion

The Committee is asked to discuss the paper and to approve the remediation activity and next steps which are:

- to complete the remediation activity on an expedited basis in coordination with the Post-Conviction Disclosure Exercise and Historical Shortfall Scheme Activity;
- for the legal team to conclude the agreed actions in respect of the assessment of all boxes stored at Oasis, on behalf of Post Office; and
- for the Group Executive (GE) to agree overall data governance accountability;

for onward submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

The inappropriately archived branch files issue has previously been raised at the Risk & Compliance Committee (RCC) and ARC meetings in September 2020.

Executive Summary

The paper addresses the situation in respect of the discovery of inappropriately archived branch file documents whilst gathering information for responses to data requests from applicants to the Historical Shortfall Scheme ("HSS"). It provides an update on the root cause analysis ("RCA"), remediation activity and legal assessment of the Historical Matters-related and Starling implications arising from the issue.

Increasingly management of data, in all formats, is a critical matter for all businesses. This paper notes the current, decentralised approach to data management in Post Office and recommends that clearer accountabilities be allocated across the business

Questions addressed

1. What was the RCA for the inappropriately archived branch files issue?
2. What is the legal assessment of the implications for Historical Matters?
3. What is the legal assessment of the implications for Starling (the "worker" claim)?
4. What remediation actions have been / are being taken?

5. What is the legal assessment of the implication for GDPR/ DPA (are we compliant)?
6. What is the legal assessment of the implication for DSARs? (has/is POL responding to these compliantly?)
7. What is the status of data governance in Post Office today?

Conclusion

1. Concerns regarding data management in Post Office have arisen as a result of the discovery of a number of archived branch files which had neither been structured nor indexed appropriately. A comprehensive remediation plan has been put in place and, subject to approval from the Committee, will be rolled out in Q3 on an expedited basis, in coordination with the Post-Conviction Disclosure Exercise and Historical Shortfall Scheme Activity.
2. To ensure that Post Office complies with its ongoing duty of disclosure as part of the GLO "post-conviction disclosure exercise ("PCDE"), the recommendation is for external lawyers to review the indices of archived boxes stored on Post Office's behalf by Oasis, by conducting key word searches, and dip testing both indexed and unindexed boxes. The dip sampling exercise will then determine the extent to which any further disclosure needs to be made (e.g. if the contents of the dip sampled boxes do not contain disclosable material, then no further review may need to be undertaken; if however they do contain disclosable material then it may be appropriate to widen the sample under review).
3. As the Historical Shortfall Scheme ("HSS") is a voluntary scheme, Post Office does not have any procedural legal obligations to review material. However, in exercising its duty of good faith to Postmasters, Post Office is taking reasonable and proportionate steps to identify sources of material which are relevant to an application and will be following the same search and dip testing processes as for the PCDE.
4. Post Office's disclosure obligation in Starling is [redacted]
5. To ensure that the GLO and Starling teams are sighted on relevant Post Office data (and therefore to mitigate against a similar issue occurring again) the following activities are planned / in progress:
    a. All branches will be contacted via letter and asked to check and disclose all records being held locally that should be archived, with updated procedural documents provided outlining the process for archiving.
    b. Data Property Services and Network are working together to identify the data owners of the boxes already at Oasis which do not have indices and to get the indices completed when an assessment against GDPR compliance will be made.
    c. The Compliance Director will circulate to Data Owners, as the accountable people for record retention, copies of the retention schedules and remediation logs and instructions on how to bring up to date. The retention schedules will also be shared with the external lawyers, so as to ensure they are comfortable that all relevant

POL00423571

records held by Post office have been made available to them.

d. A communication from the General Counsel will be sent to the Leadership Council on the obligation to assist and put in place measures to address any outstanding issues identified by the Records Retention Programme and included in Business remediation logs. Following which attestations will be requested from the Data Owners that:

   i. Retention Schedules they are accountable for are accurate and up to date and any new data sets being flagged to the Head of Cyber Compliance in accordance with the Document Retention Policy.

   ii. The remediation logs are being worked through to close any gaps.

   iii. Minimum Control standards are in place.

6. Post Office must conduct reasonable and appropriate searches for information requested as part of the DSAR process within GDPR. For the purpose of HMU requests, the HSS data team have cross-referenced system data and conducted extensive searches in ten different sources. This is time consuming but ensures Post Office is not in breach of statutory obligations in respect of handling DSARS as these searches would be deemed to be reasonable and appropriate.

7. Currently the Legal Hold Order that is in place in relation to the GLO and HMU work is a recognised exemption to the requirement to hold information for no longer than is necessary. The remediation logs from the Record Retention programme obliges the business to have processes in place to delete all expired information once the hold order is removed.

8. In respect to Post Office handling of FOI requests, the legislation obliges Post Office to conduct reasonable and appropriate searches to locate in-scope information. FOI allows Post Office to apply a time and cost exemption to locate the data, should these be exceeded then the request can be rejected, including where searches are prolonged due to poor record keeping practices. Therefore, as long as Post Office can evidence that the necessary searches have been conducted then the risk of ICO intervention is low.

9. Data Governance in Post Office is managed through a number of different controls and accountabilities. This is a decentralised approach and there is no single record depository that enables the business to quickly identify and manage the data it holds. It is recommended therefore that Post Office seeks to establish a single accountable unit for data governance, supported by oversight from the CISO for data security and Compliance for personal data protection.

POL00423571

Report

What was the RCA for the inappropriately archived branch files issue?

1. As previously reported in the September 2020 RCC, the data team, working on the HSS, identified inappropriately archived boxes held at Oasis[1], our archive provider, which might have relevance to the HSS DSARs. However, it was not possible to determine quickly what was held in those boxes and whether the material in them was of any relevance to the DSARs.
2. Initial investigations on a small sample suggest that branches have not being following the archiving processes for branch records.
3. When a branch closes/closed an archiving process is meant to be followed. This involves empty file boxes being sent to the branch and a list of requirements for archiving to be completed. A list of contents is meant to be put in the archive box. Other than branch name and FAD code, there does not appear to have been any external indication on the contents of the box and Oasis do not open boxes at site.
4. The contents of the boxes may contain any branch balancing hard copies, Trading statements, daily and weekly reports. They may also contain HR files such as P250 assistant verification and contractual information on the agent/postmaster.

What remediation actions have been / are being taken?

5. Where the HSS data team have requested personal data for DSARS from incorrectly indexed boxes, additional searches have been conducted with the business area to locate the personal data. To date, the HSS team have been able to obtain the required data through cross referencing across multiple systems data and combining information and provide Post Masters with shortfall information.
6. Processes have been developed to ensure that we can meet our obligations or prove that we have conducted the appropriate searches to meet the 'reasonable and appropriate' test.

Digital data / MI:

7. The Data Governance team in IT is conducting a review of the digital data/MI RACI.
8. There are 3 clear priorities to be progressed if Post Office is to manage its data asset with the same degree of rigour as it does other enterprise assets. These priorities are:
   a. 'Fix the foundations' – correct the weaknesses in core data management disciplines and governance
   b. Validate and deliver prioritised MI requirements to the business
   c. Confirm the approach and plan to progress the overall information strategy (including development of a more detailed set of requirements, operating model, and business case and to transition to a new MI organisation).

Branch document retention and archiving:

9. A plan is being implemented to ensure that any documents held in branches that should be archived in accordance with the archive standards are disclosed, properly indexed and submitted to Post Office's offsite storage (Oasis Records Management). Also, activity is being undertaken to ensure that processes for record retention in Post Office, as

[1] It is understood that the universe of boxes stored at Oasis is c103,000.

POL00423571

defined in the Document Retention programme are being actioned. A summary of the plan is as follows:

a. All branches will be contacted via letter and asked to check and disclose all records being held locally that should be archived

b. Area and Regional Managers will be briefed to support this process

c. These communications will include updated procedural documents (which are being updated by the Property and equipment Management Team) outlining the process for archiving and what should and should not be included in boxes sent to archives. This will ensure that the lifecycle and the integrity of the data is maintained through to deletion.

d. Property Services and Network are working together to identify data owners of boxes already at Oasis that do not have indices and to get the indices completed.

10. Document Retention process in back office functions:

a. A communication from the General Counsel will be sent to the Leadership Council on the obligation to assist and put in place measures to address any outstanding issues identified by the Records Retention Programme and included in Business remediation logs. This communication will be issued once the revised structures are confirmed, post 13th November 2020.

b. The Compliance Director will circulate to:

i. Data Owners, as the accountable people for record retention, copies of the retention schedules and remediation logs and instructions on how to bring up to date.

ii. Data Owners, copies of the Data Retention and Deletion Policy, Protecting Personal Data policy and Cyber Information and Security Policy to ensure that all control standards are being complied with and identify gaps that exist.

iii. Internal and external lawyers, copies of record retention schedules for analysis. This will enable the lawyers to be confident that all records held by Post Office have been considered for Historical Matters.

c. Attestations will then be requested from the Data Owners that:

i. Retention Schedules they are accountable for are accurate and up to date and any new data sets being flagged to the Head of Cyber Compliance in accordance with the Document Retention Policy

ii. The remediation logs are being worked through to close any gaps

iii. Minimum Control standards are in place

11. GDPR considerations:

a. The RCA has now identified a number of boxes that have no indexes. These boxes are to be considered from a GDPR perspective to ensure compliance with obligations. This, in itself, does not constitute a breach of legislation, which would only occur if we;

i. Knowingly withheld personal data that had been requested as a result of a DSAR. Post Office have conducted extensive searches for personal data requested by applicants to the HSS. There are currently ten cross-business searches conducted to locate information which will assist in the completion

POL00423571

of applications to the scheme. This level of examination would meet the criteria of reasonable and appropriate as required by GDPR.

ii. Hold information longer than is necessary. The legal hold order that is currently in place allows Post Office to retain that information until the order is removed. Given that these files hold information relating to Branches and Postmasters, and is therefore in scope of the hold notices, then we are confident that this does not constitute any breach of GDPR obligations.

b. Should any unindexed boxes be found to contain personal data that should have been included in a 'release all data' DSAR then Post Office would provide that information to the requestor, if disclosable. It should be noted that outside of HMU we have never had any reason to search branch file information to service a DSAR.

c. As part of the remediation plan, Data Protection will work with Property Services and Network teams to;

i. identify the owners to allow the correct record retention schedules and indexes to be applied. As there is no evidence that any individual has suffered and harm, damage or distress then this is not a notifiable incident to the ICO. Key to this is demonstrating that remediation plans are progressed.

ii. consider whether any recent DSARs have been processed that would have included requests for information from this source (Please note a search of all non-HMU DSARs received in the last three years would not have required any search of these boxes. For HMU DSARs we have been able to locate information requested by alternative means).

What is the legal assessment of the implications for "Historical Matters"?

12. With respect to past prosecutions brought as a private prosecutor, Post Office owes a post-conviction duty to disclose material to defendants that might cast doubt on the safety of their conviction, and to make enquiries where there is a real prospect that the enquiry would reveal such material. The method by which these duties are discharged is through a "post-conviction disclosure exercise" ("PCDE").

13. With respect to the Historical Shortfall Scheme ("HSS"), Post Office does not have any procedural legal obligations concerning disclosure as it is a voluntary scheme. However, following the GLO Common Issues Judgment, Post Office owes a duty of good faith to postmasters requiring it to deal with postmasters fairly and transparently, a principle reflected in the HSS's Terms of Reference and Q&A's. Post Office is addressing this by taking reasonable and proportionate steps to identify sources of material which are relevant to an application (the standard adopted in conventional civil court proceedings).

14. In addition to this, Post Office has an obligation to conduct reasonable and appropriate searches for Personal Data requested through the DSAR process. It is a reasonable assumption that if the archived boxes were indexed correctly then these would be considered 'relevant filing systems' for the purpose of GDPR and in scope for future searches. However, given that the information required for the HSS DSARS has been collated through other cross business searches then there is no breach of the GDPR.

15. Post Office initially addressed the impact by reviewing available indices to identify boxes which might contain material relevant to the PCDE or HSS, and extract from those boxes any material required to be disclosed as part of the PCDE, or which would be relevant to the consideration of an HSS application.

POL00423571

16. Subsequent to receiving approval from the Historical Matters Steering Committee, for both the PCDE and HSS, Post Office is addressing the issues identified through:

    a. Key word searches being applied (or in the case of previous searches, re-run) across the expanded set of indices to identify boxes which may contain relevant material, which will then be reviewed to identify relevant material;

    b. Undertaking a "dip sample" exercise of a statistically representative random group of indexed and unindexed boxes (c.100 of each) to assess the extent to which they contain material relevant to the PCDE (which would be disclosed as part of the PCDE) or the HSS work (which would be considered as part of the investigation into a specific application).

    c. The results of the dip sample will inform the next steps that may need to be taken with respect to the remaining boxes (e.g. further reviews may be required if the sample identifies significant volumes of material relevant to the PCDE and/or HSS).

17. These steps (which are being carried out on an expedited basis in coordination with the PCDE and HSS), combined with the remediation actions described above, will give confidence that Post Office has addressed the obligations described above to review known sources of materials for the PCDE and HSS.

What is the legal assessment of the implications for Starling (the worker claim)?

18. Post Office's disclosure obligation in Starling [redacted]

19. [redacted]

20. [redacted]

21. [redacted]

22. [redacted]

POL00423571

What is the status of data governance in Post Office today?

23. Data governance in Post Office is managed through a number of different controls and accountabilities. This is a decentralised approach and there is no single record depository that enables the business to quickly identify and manage the data it holds.

Existing key controls

24. POL needs to manage its data to operate appropriately and effectively. In order to do this a number of controls both at the enterprise, group and function level have been established outlining levels of accountability and responsibility.

25. These controls are set out, principally, through the following policies:

    a. Cyber & Information Security Policy (principally a technical IT policy)

        i. Acceptable use standards

        ii. Access controls standard

        iii. Asset management standard

        iv. Encryption standard

        v. Information classification standard

        vi. Network [IT network] security standard guidelines

        vii. Platform security guidelines

        viii. Platform security standards

        ix. Secure development lifecycle guidelines

    b. Document Retention and Disposal Policy

        i. The Record Retention programme, completed in Q4 2019/20, identified the Data Owners and data held, which was put into the record retention schedules

        ii. A GE re-prioritisation exercise in February 2019 resulted in the Record Retention Programme's funding being halved (from £1.6m down to £0.8m) and remediation being de-scoped, save for providing IT solutions to high-risk areas to automate the adherence to these schedules for Telecoms (Fujitsu), POI (Home insurance, pricing & analytics, Travel insurance, MI and HR), the Brands database and HR (Success factors & SAP).

    c. Protecting Personal Data Policy

26. The Document Retention & Disposal and Protecting Personal Data policies set out the control standards that Data Owners must ensure are adhered to. The key controls are:

    a. As part of the design of a new product or service, or where a product or service is being updated, product or service risks must be considered, mitigated and documented before completion of design phase. This must include updating of any related Document Retention Schedules;

    b. The integrity and accuracy of data must be ensured at the point of collection.

    c. Data Owners are also responsible for maintenance and adherence of their retention schedules. All Data Owners must ensure that the retention schedules for their area are up to date. This is especially important when changes are being implemented to business processes.

POL00423571

d. Data Owners must understand the complete information lifecycle (creation, capture, index, manage, access, retrieve, administer, repurpose, share, retain, dispose, preserve) for all data within their sphere of control.

e. Data Owners must ensure that they have defined the storage requirements for the data under their sphere of control, and that this has been documented and agreed. This particularly applies where encryption is required. This is a field within the retention schedule.

27. Each team within each business unit has a record retention schedule in place. This schedule details the records they create / hold, where they are stored, their classification, retention period, storage instructions and end of period action.

28. These schedules are stored centrally on the CISO SharePoint Site and were produced by the Record Retention Programme.

29. Once produced, each schedule was signed off and approved by the relevant GE-1 member (and supporting team) with responsibility for remediation, adherence and keeping them up to date handed over to the relevant GE-1 member(s), in accordance with the Group Retention and Disposal Policy. This responsibility was communicated to each 'Data Owner'.

Next Steps:

30. Completion of the remediation activity on an expedited basis in coordination with the Post-Conviction Disclosure Exercise and Historical Shortfall Scheme Activity

31. Lawyers to conclude the actions in respect of the assessment of all boxes stored at Oasis, on behalf of Post Office.

32. GE to agree which business function has overall accountability for data governance, supported by oversight from the CISO for data security and Compliance for personal data protection.

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Procurement Governance & Compliance Report	**Meeting Date:**	12 November 2020
Author:	Barbara Brannon, Procurement Director	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to review the report and note that no Procurement Risk Exceptions submitted to the Post Office Limited Board since September 2002 and to consider and give direction in respect of the contracts in the Procurement pipeline which are high value and at risk of being awarded or extended non-compliantly.

The Committee is also asked to note the alteration in governance approved by ARC and to advise on preferred governance processes in respect of subthreshold risk exception requests.

Previous Governance Oversight

- July 2020 - Quarterly Risk Report
- September 2020 – Board Report

Executive Summary

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

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

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

In March 2020, Post Office Board requested prior approval of all Exceptions. This was revised in September 2020 to above threshold Exceptions >£189k only in a revision to existing governance. From November 2020 sub threshold exceptions will be reported retrospectively to RCC and to ARC.

A Procurement Risk Exception Note is required to accompany all Exception Requests and a Legal Risk note for requests >£189k.

Questions addressed

1. *How many and what types of procurement risk exceptions have occurred in the past quarter?*
   Since the last Board report at the end of September there have been no Procurement Risk Exceptions submitted to Board for approval.

   We currently have a lapsed contract with our auditors, PWC which is an internal governance breach. A compliant extension option exists to extend but they are currently working at risk preparing an audit plan for 2020/21 while commercial terms are negotiated.

2. *What are we doing about it?*
   Active reviews continue with Business Units with the highest values relating to non-compliance.

   Our overall non-compliance value has reduced from £27.7m in July to £9.2m in November.

   A number of material risks including the retendering of our Payments Processing services [Global Payments] have been retendered, awarded and closed. The Customer Database and Marketing Services [RAPP] process is in closing negotiations and will be resolved before Christmas with a significant Opex saving.
   A visual breakdown on all Open incidents at 5/11/20 is available in Appendix 1.

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

   a) £10m. **EUC**

   A project has been initiated to re-procure End User Computer services for both Branch and Colleague Services. The project has been delayed and re-baselined due to Covid resource constraints. The revised plan targets April 2021 to award a new provider for Colleague Services with Branch services the subject of a separate tender process. This process will complete by end of May 2020 without further slippage. In both cases, the termination assistance period will have commenced prior to award. The project is currently gathering requirements to go to market however, the exit assistance period was the subject of an earlier Legal Risk Note which has been updated and is attached in Appendix 2.

   b) £1.5M. **Cheque Clearing**.

   A risk exception was submitted to Board in June 2020 to extend our cheque clearing services with Barclays. An undertaking was made to retender the service within the period of the 12 month extension. Due to resource constraints over the summer period, the project started in earnest in September with a Project manager assigned in late

October. A review of the market has indicated that an OJEU process will be required for an As Is solution. There is just adequate time left to do this, however, the gross costs of the expiring contract *combined* with the RMG delivery costs make this a loss-making service for POL.
A discussion paper is appended which sets out the challenges of identifying an appropriate solution, and therefore the procurement process and associated timeline. An alternative solution would necessitate a further 6 month contract extension in order to adequately define requirements, allow for a process to be run, and a possible transition process. Our external contract obligations in respect of cheque clearing for Banking Framework require an 18 month extension.

c) **CLOSED. £189k/aggregated £1.2m. Pipeline risk on Swindon software.**

This has been resolved as of 11/11. A CAF process is now underway.
Procurement have been negotiating with an IT vendor for some time to bring a legacy software contract into compliance via a reseller. The software supports our Swindon operation and termination is not an option at present. Following acquisition by a US firm, they have withdrawn from the process at short notice. Escalations are proving productive and we are hopeful of resolving before ARC/Board. A PREN and Legal Risk Note are attached for review within Appendix 2 in case this becomes necessary.

d) **TBC - Common Digital Platform (CDP) Disaggregation.**

Rather than procure a like for like service for application support and development IT are using this opportunity to align CDP with the future IT strategy and disaggregating the service. Hosting is already in the cloud and will compliantly transfer to the Back Office contract before transferring to the POL CoE for Cloud in due course. Options for application support and development [tendering certain pieces, moving non-customer facing components compliantly into the existing Back Office Accenture contract, and insourcing some elements] are under review with IT and Legal.
At present the application support and development services are unlikely to have been completely retendered or moved to other existing PCR compliant contracts by December as proposed to GE and Board and there are concerns in respect of resourcing and funding.
The view, however, is that this will have been completely achieved before revised contract end date in June 2021. The vast majority (by value) is expected to have been completed by the end of January 2021 as set out in the original Board paper.

4. *What are the key changes in the revised governance agreed with ARC in September?*

Following review of the annual Procurement compliance report in March 2020, the Audit and Risk Committee [ARC] have requested a revised approval process for all Procurement Risk Exceptions.

A revised process was been discussed with ARC in September and the following key changes made:

1. Subthreshold exceptions will be retrospectively reported to RCC and ARC every two months. This will become a standing item at ARC rather than an annual report. ARC will review this position within 6 months. A commercial, pragmatic approach to such risk was endorsed by the Board in September.
2. Above threshold risk exceptions [>£189k] will continue to require prior approval from Board
3. Above threshold Pipeline risks, sourcing options and recommendations*, progress reports on for material procurements, and bi-annual strategic pipeline report will continue to come to Board.
   *It is particularly noted that Board wish to understand the available commercial options, procurement routes and associated risks [both commercial and of legal challenge]; and proposed evaluation criteria with sufficient time to discuss and influence if desired.

Prior to March 2020, sub threshold exceptions were approved by the relevant GE member and SLP; and the Procurement Director. These exceptions were logged, with mitigation plans to bring into compliance where exceptions were made for an ongoing requirement rather than a one-off event.

RCC are asked to advise on preferred governance processes in respect of sub-threshold risk exception requests.

Conclusion

Risk Exceptions are subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk.

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

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

Report

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

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

POL00423571

Non-compliant awards may be made for a number of reasons at the Post Office.

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

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

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

A full explanation of the individual compliance breaches for direct awards over £189k [previously £164k & £181k] threshold is attached in Appendix 1. Each entry details the nature of, and the value of the breach. The threshold is altered every two years based on the FX rate between GBP and the Euro.

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

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

9. How many of the breaches were approved in advance and how many retrospectively?
All contracts entered into during this period were compliant with internal governance processes on contract and commercial review.

10. Why were the approvals given?
The rationale for approval is relevant to the individual service and is detailed within Appendix 1.

11. What were the unapproved, material breaches?
There were no unapproved, material breaches during this period.

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

POL00423571

Risk Assessment, Mitigations & Legal Implications

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

14. Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

15. The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

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

POL00423571

Appendix 1 - All Open Material Incidents

Date	Procurement Category	Function	GE Member	Supplier Name	Value	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
10/01/2018	IT Software	Retail & Franchise	Amanda Jones (interim)	NCR	£ 1,800,000.00	In flight	PCR OJEU level	Annual maintenance and support previously provided under Regulation 32 exemption for IPR. Cover is now expired and a compliant route found. Negotiations are underway.
15/06/2019	Marketing	Marketing & Brand	Emma Springham	RAPP/ CODE	£ 1,000,000.00	In flight	PCR OJEU level	OJEU expired
23/12/2019	PR	Corporate Affairs & Comms	Richard Taylor	Cardew Group	£ 377,860.60	Pending	PCR OJEU level	Direct award - no procurement engagement
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	Abcomm	£ 42,000.00	None	Medium threshold	Direct award - no procurement engagement
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	9XB	£ 30,000.00	None	Medium threshold	Direct award - no procurement engagement
30/12/2019	Comms, R&I & PR	Corporate Affairs & Comms	Richard Taylor	Kantar	£ 52,000.00	Pending	Medium threshold	Direct award - no procurement engagement
30/12/2019	Market Research	Corporate Affairs & Comms	Richard Taylor	AB Publishing	£ 100,000.00	Pending	Medium threshold	Direct award - no procurement engagement
27/03/2020	IT Software	IT	Jeff Smyth (interim)	Interchange	£ 292,995.00	In flight	PCR OJEU level	POL inherited the Galaxy system and support contracts from Royal Mail was part of, then descoped from compliant OJEU tender for Back Office in 2015
29/03/2020	IT Software	IT	Jeff Smyth (interim)	CSM Accent	£ 30,000.00	In flight	Medium threshold	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	IT Software	IT	Jeff Smyth (interim)	JDW	£ 169,000.00	In flight	PCR OJEU level	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	Media	Marketing & Brand	Emma Springham	Carat	£ 1,873,000.00	In flight	PCR OJEU level	Contract extended to cover OJEU process time line which has been extended
29/03/2020	Marketing	Marketing & Brand	Emma Springham	CACI	£ 392,380.00	None	PCR OJEU level	No frameworks and no appetite in business for full OJEU. Limited other suppliers who have access to the market or simillar software. Software Reseller not an option. Approved by Board March 2020

Strictly Confidential

POL00423571

Date	Procurement Category	Function	GE Member	Supplier Name	Value	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
21/05/2020	Supply Chain	Operations & Supply Chain	Alisdair Cameron	Kings Secure Technologies	£ 90,000.00	In flight	Medium threshold	Interim contract put in place while POL exits ATM terminals from WHSmiths. Board approval granted
21/05/2020	Supply Chain	Operations & Supply Chain	Alisdair Cameron	Cardtronics	£ 300,000.00	In flight	PCR OJEU level	Interim contract put in place while POL exits ATM terminals from WHSmiths. Board approval granted
01/06/2020	Professional Services	Corporate Affairs & Comms	Ben Foat	KPMG	£ 107,000.00	None	Medium threshold	Selected due to their prior knowledge and to limit number of firms involved in sensitive matters. Board approval granted.
25/06/2020	IT SaaS	Marketing & Brand	Emma Springham	Splash	£ 42,000.00	Pending	Medium threshold	Re-procurement exercise was underway but due to Covid-19 and budget restraints this exercise had to be put on hold. Also require input from solution architect and workload has prevented this
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley	Barclays	£ 1,600,000.00	Pending	PCR OJEU level	Contract extended with Barclays beyond the limits the OJEU allowed.
25/06/2020	Banking Services	Retail & Franchise	Owen Woodley	Barclays	£ 500,000.00	Pending	PCR OJEU level	Postal Orders/Camelot cheques. Service originally with Co-Op. they terminated the contract in order to exit cheque clearing market. Barclays stepped in to pick up service as very similar to cheque clearing. Work underway to review if it can be tendered alongside the main cheque clearing services.
10/07/2020	Public Affairs	Corporate Affairs & Comms	Richard Taylor	Lexington Communications	£ 173,062.58	None	Medium threshold	Direct award for GLO related PR services. Board approval given.
10/07/2020	Marketing	Marketing & Brand	Emma Springham	CPA global	£ 72,482.00	Pending	Medium threshold	Direct award - trademark services. Contract transferred across to Marketing but compliance status was unknown and it was too late to retender. WIP for 2021
10/07/2020	Professional Services	Finance	Alisdair Cameron	Lexus Nexus	£ 36,238.63	Pending	Medium threshold	Threshold breached - was previously compliant
02/11/2020	Auditors	Finance	Alisdair Cameron	PwC	£ 1,200,000.00	Pending		A compliant contract is in place but has lapsed during contract negotiations. 1-2 year extension should have been signed before October. This hasn't happened as we have not agreed fees for next years audit with PwC thus far.
01/09/2020	Professional Services	Commercial	Owen Woodley	Grant Thornton	£ 151,000.00	None	Medium threshold	Urgent financial support required in relation to HPBB sale
					£ 9,231,018.81	excluding Audit Value		

Strictly Confidential

POL00423571

Appendix 2 – Procurement Risk Exception Note(s)

PREN 20 - PREN20 EUC Procurement Risk Exception Form Pipeline v1.1 UPDATE 04 Nov. 2020

PREN26 – PWC Pipeline Risk Audit Note

Discussion paper - PREN18 Barclays Bulk Cheque Processing Contract November Update 2020

For reference

PREN18 Board Paper Bulk Cheque Processing Contract June 2020

PREN18 Legal Risk Note, June 2020

POL00423571

Procurement Risk Pipeline Form

1.Business area or Project Details					
Date Raised	**Original submission 02 July 2020 updated 05 November 2020**	**Business Area/Project**	**IT/ End User Compute**	**GE Member**	**Jeff Smyth**
Raised By	**Rob Whitehead**	**GE-1 Exception Owner**	Gary Walker	**Value of Award**	**£6.1m (£0.6m BAU service costs during TAP plus £5.5m transition costs)**
				Total Value	**£66m full life costs April 2015 – April 2021**

2.Risk Details					
Risk Title	End User Compute – Termination Assistance/Exit Services Risk				
Risk Type (New/ Contract Extension)	**Extension** **Termination Assistance Period**	**Exception Category**	Regulation Breach	**Exception ID**	*To be provided by Procurement*
Detail of contract at risk of exception request and its purpose.	This note is to explain the residual risk in relation to using a contractual mechanism called the Termination Assistance Period within the Post Office Limited (POL) End User Computing (EUC) with Computacenter (CC). The contract covers provision and support for all of POL's Colleague, (e.g. Laptops, printers, central login mechanism, etc.), Branch end user compute environments (e.g. Counter hardware that executes Horizon, receipt printers, PEDs, etc.) as well as Shared Services (e.g. components used by both Colleague and Branch such as Microsoft Active Directory). This contract has been in place since 30 April 2015 and POL has already utilised all available compliant options for extension. Our contract will end on the 29 April 2021 and this end date is known by other providers of similar services (DXC, Accenture and, SCC). Based on the remaining time on the CC contract, the time to prepare for and then run a competition(s), followed by the time to transition services, it is not possible for POL to exit and transition all services before the 29 April 2021 contact end date, regardless of which strategy is utilised. POL will therefore need to utilise a contract mechanism called the Termination Assistance Period (TAP). The TAPs primary use is to allow Computacenter to continue to deliver live services whilst a new incumbent (or POL) transitions services away. POL must give CC at least 4 months notice, by 29 December 2020, to commence services under the TAP which can then run for a maximum of 24 months, with an option to extend the Termination Services for a further 6 months.				

POL00423571

Procurement Risk Pipeline Form

<table>
<tr><td></td><td>The TAP must be used for exit activities only and cannot be used to simply extend or transform the existing service.

The TAP was put in place during the preferred bidder stage of the procurement for the current contract and had not been part of negotiations with the wider market.

Legal advice was provided in relation to that risk at the point of approval of the EUC Agreement. This advice identified the risk as low as transition services over the TAP timescales are not unusual for an ICT contract of this type and because it was envisaged that, at the time of the use of the TAP, procurement(s) would be underway for replacement services and so interested bidders would be motivated not to challenge.

This means that by April 2021, POL must be demonstrably and overtly in the process of exiting the existing contract.

The procurement plan for replacing the current CC End User Compute contract is to split the existing contract into 3 parts, each procured separately.

Current planning to support EUC IT strategy is three procurements, see key milestones below:

<table>
<tr><th>DELIVER Phase Tasks (continued)</th><th>Date</th><th>Status</th></tr>
<tr><td>Colleague Print Contract Award (Direct Award)</td><td>17/03/2021</td><td></td></tr>
<tr><td>Colleague EUC Contract Award</td><td>16/4/2021</td><td></td></tr>
<tr><td>Colleague Print Transition Complete</td><td>29/04/2021</td><td></td></tr>
<tr><td>Commence TAP support with CC</td><td>30/04/2021</td><td></td></tr>
<tr><td>Branch EUC Contract Award</td><td>20/05/2021</td><td></td></tr>
<tr><td>Colleague EUC Transition complete</td><td>26/11/2021</td><td></td></tr>
<tr><td>Branch EUC Transition complete</td><td>31/03/2022</td><td></td></tr>
<tr><td>TAP Support with CC ends</td><td>31/03/2022</td><td></td></tr>
<tr><td>Programme Closure /CLOSE Gate</td><td>19/05/2022</td><td></td></tr>
</table>
</td></tr>
<tr><td>How long may asking the business to tolerate /accept this risk? (duration)</td><td>Start date 30 April 2021 End Date(s) 20 May 2020</td></tr>
<tr><td>What commercial options have been considered?

Why is the chosen option now at risk of non-delivery?</td><td>At its meeting on 01 July 2020 GE endorsed a recommendation to compete the procurement exercise for new contract(s), (3yr + 2yr), before April 2021 with transition completed by Sept 2021.

This strategy provided the greatest opportunity for optimising savings (due to deal size) and via a structured procurement. This requires an investment of £6.11M and is the existing strategic direction (as of December 2019), albeit with greater utilisation of the TAP than originally envisaged due to Covid19 delays. This would allow us to proceed to market in a standard, structured fashion with a view of transitioning services to a new supplier.

This potentially offers only lower (but predictable) in year OPEX savings which are currently estimated at approximately <£750K. There is however a greater possibility of obtaining on-going OPEX savings post 2022/23 (assuming 21/22 is lost due to transition charges) as a result of the tendering activity. This could be in the region of £1.5M pa post transition and transformation.</td></tr>
</table>

POL00423571

Procurement Risk Pipeline Form

<u>EUC Reprocurement Summary (Update since June Board)</u>

The EUC programme has had several issues with resources and delayed decision making, in particular:

- Delays have occurred in decision making for the EUC strategy and target operating model for Branch and Colleague EUC Services which has had a knock-on effect for the associated procurement strategy / routes to market.
- Delays occurred with regards to programme approvals and the DELIVER gate artefacts, in particular, the required business case to progress from the PROVE phase. This is in part due to challenges with multiple changes to programme resources, in particular the PM role.
- As a result, in July/August the Prove phase was re-baselined and a PROVE CR approved at IC on 24th August which included additional PROVE funding approval of £421k to January 2021.

Progress against revised PROVE Plan:

- The programme is now progressing on-track to the re-baselined plan and budget with the DELIVER Business Case signed off and submitting to PRB 21/10, tracking to approval at 24th November POL Board.
- The programme is now resourced and progress towards the Pre-Market Engagement event is being made with a Pre-Market Engagement Prospectus and Engagement Day (virtual Teams meetings), however there are delays in approval for this activity.
- Creation of the Print Specification and Direct Award assessment criteria, as well as preparation of the Colleague EUC Further Competition pack is underway.
- The business case has re-baselined and re-evaluated resources needed to complete preparations for issuing Further Competition Invitation to Tenders (ITTs) resulting in a reduction of FY20/21 forecast of £127k forecast for the current Financial Year.

Key Plan Milestones	Due Date
Pre-Market Engagement Complete	20/11/2020
Finalise Print Spec and Direct Award Assessment	20/11/2020
Finalise Colleague EUC Further Competition Pack	10/12/2021
Issue Colleague EUC Further Competition to market	14/12/2021
Notice requesting Termination Assistance	29/12/2020
Colleague Print Contract Award (Direct Award)	29/01/2021
Finalise Branch EUC Further Competition Pack	10/02/2021
Issue Branch EUC Further Competition to market	11/02/2021
Print Contract Start	01/04/2021
Colleague EUC Contract Award	16/04/2021
Colleague Print Transition Complete	29/04/2021
Colleague EUC Contract Start	30/04/2021
Commence TAP support with CC	30/04/2021
Branch EUC Contract Award	20/05/2021
Branch EUC Contract Start	21/05/2021
Colleague EUC Transition complete	26/11/2021
Branch EUC Transition complete	31/03/2022
TAP Support with CC ends	31/03/2022

POL00423571

Procurement Risk Pipeline Form

What is the recommendation from Procurement? [Include alternative approaches and detail risk mitigation options if available]	Procurement fully supports the use of TAP to conclude the procurement activities which have already commenced within the market. As per the Legal Risk Note from Ashfords LLP dated 3rd November 2020, there is a residual risk based around how the TAP was included in the contract during the preferred bidder stage. This risk remains. There are several factors mitigating the residual risk of challenge: • Suppliers who might be aware that TAP was not part of the original contract will be included in competitions for the replacement services so less motivated to challenge. • Any challenge would be limited to damages rather than ineffectiveness and lawyers are likely to advise against such a claim for a short 'breach' whilst the procurements and completed. • The OJEU Contract award notice set out the termination assistance will be provided after the termination date • The total contract value to date is £66m and the further spend will not be close to the maximum value of £300m in the OJEU • Even if the TAP could not be used to provide the Services post termination, it is likely that the provision of the Services would fall under the ability to modify a contract under Regulation 72(1)(b) of the Public Contract Regulation 2015 in any event as a means to extending the services. Any risk of challenge is further mitigated by POL requesting Termination Services, including the provision of BAU services during the TAP. To obtain the Termination Services POL must request them by way of a Termination Assistance Letter. The Termination Assistance Letter must to be sent to Computacenter by 29 December, not less than four months before the end date of the contract.					
PCR Risk Mitigation	**Yes, as per Legal Risk Note**			**To commence re-procurement as soon as possible.**		
PCR Risk Level *[shade as appropriate]*			**Low**	**Legal Risk Note supplied**	**Yes**	

3. What controls are in place, actions completed or work in progress to mitigate the risk?		
Control or Action detail to prevent a Risk Exception and/or to ensure it is constrained to the minimum period of risk possible. Include PCR Risk mitigations.	**Target Date**	**Action or Control Owner [business / procurement]**
Governance: Owing to capacity issues, the Programme is behind on governance in terms of SteerCo approved decisions, which represents a risk to the scope being presented in the Business Case. The SteerCo needs to be urgently re-established and working decisions need to be formalised/approved.	October 2020	SteerCo to be re-established to provide governance and direction for the project
TAP: The revised timeline results in the planned Branch Contract Award on 20th May 2021 and transition commencing in late June, after the expiry of the current CC contract. This will require a short period where TAP will be used to continue current service delivery to Branch prior to award and transition. This period is considered to present a low risk of challenge owing to the Branch procurement being substantially complete and Colleague /Colleague Print being transitioned at that time. However, it does represent a risk to POL of challenge	December 2020	Complete the requirements and procurement documentation. This will ensure that the procurements

POL00423571

Procurement Risk Pipeline Form

		run to the revised project plan.
TAP Changes: Owing to the timing of the procurements, supplier bids will not have been received with details of transition plans/activities when POL needs to have issued the Notice requesting Termination Assistance (29th December 2020). This is likely to result in changes needing to be made to TAP when supplier responses are received in Spring 2021. Under the 2019 Letter of Extension, the Services and Termination Services provided according to Termination Assistance Notice may be amended using the Change Control Procedure during the TAP, including to extend or reduce any time periods for the provision of any such Service or Termination Service. POL's right to terminate the TAP early for convenience after expiry of the Agreement would not apply as the clause does not survive expiry of the EUC Agreement	December 2020	The project has modelled various transition strategies and the Termination Assistance Letter will be based on the most likely scenario

POL00423571

Risk Note

Author: Suzie Miles (Commercial) and Lucy Woods (Procurement) - Ashfords LLP Date: 03 November 2020

Summary

Post Office Limited ("**POL**") must give Computacenter a Termination Assistance Notice by 29 December 2020 at the latest to trigger a Termination Assistance Period. The TAP shall end no later than 29 April 2023. During the TAP CC shall, at the request of POL: (i) continue to provide the Services with phased transition to a Replacement Contractor; and/or (ii) provide Termination Services. While technically there is no clause entitling POL to extend the TAP, the EUC Agreement does provide that POL can extend the provision of the Termination Services and services that are the same or similar to the Services for up to 6 months beyond the TAP using the Change Control Procedure, which is akin to extending the TAP beyond 24 months. Furthermore, POL can also reduce the period of the TAP using the Change Control Procedure.

POL is only required to issue a Termination Assistance Notice to request Termination Services during a TAP. Notwithstanding this there are provisions stating that POL can request the Supplier to provide the Services during the TAP as well as the Termination Services or on its own without any Termination Services. It is therefore unclear how POL would trigger the TAP if it only wanted the Services to be continued and not any Termination Services. Our advice would be that POL still issue a Termination Assistance notice and detail any high level Termination Services that it may require at any stage during the TAP, including access to information.

Background

POL and Computacenter (UK) Limited ("**CC**") entered into the End User Computing Services Agreement on 29th April 2014 ("**EUC Agreement**"). On 29 November 2019 POL and CC signed a letter of extension to extend the EUC Agreement for a further 12-month period commencing on 30 April 2020, which means the EUC Agreement will expire on 29 April 2021 ("**2019 Letter of Extension**"). POL does not have another option to extend the EUC Agreement after this extension.

POL is considering re-procuring the services under the EUC Agreement. POL does not wish to terminate the EUC Agreement early but wants to explore the possibility of triggering a Termination Assistance Period ("**TAP**").

This note provides a summary of the (i) procurement risks and (ii) commercial risks related to triggering the TAP under the EUC Agreement.

Unless specified otherwise, defined terms under this risk note have the same meaning as under the EUC Agreement.

Commercial risk note

Term and expiry

Under clause 66.1, the EUC Agreement commences on the date of signature (the Effective Date, being 29th April 2014) (note that we have not seen a dated version of the EUC Agreement but this is as detailed in the letter of extension) and expires at the end of the Term (being the Initial Term and the Extension Period). POL does not need to take any action to effect the expiry of the EUC Agreement.

The Initial Term is 4 years from the Service Commencement Date (being 30 April 2015, as per Schedule 1) and POL has 2 options to extend the Initial Term for Extension Periods of up to 12 months each (clause 66.3).

The 2019 Letter of Extension specifies that the Term is extended to 29 April 2021.

Charges

During the TAP, POL shall continue to pay for the Services. The 2019 Letter of Extension calculated the reduction to the Charges for the Services in FY19/20 and FY20/21. POL shall additionally pay for any Termination Services, Knowledge Transfer or reasonable assistance based on the Rate Card and as agreed in advance with POL. The Charges for the Services and Termination Services shall be re-calculated for the TAP.

All outgoings and expenses, rents, royalties and other periodic payments in respect of Assets and Sub-contracts transferred to POL or the Replacement Contractor shall be apportioned between POL, CC and the Replacement Contractor, as applicable (paragraph 5.4, Schedule 8.5).

Termination Assistance Period

Duration

The TAP shall end no later than 29 April 2023 (not longer than 24 months after the expiry of the Term (Schedule 1, Schedule 8.5 and 2019 Letter of Extension)), but POL has the right to extend the Termination Services for another 6 months beyond the TAP.

The Services

During the TAP, CC is required to continue to provide the Services to the required Service Levels and no degradation in the standards of the Services (clause 69.1; paragraph 6.1 Schedule 8.5).

Termination Services

CC shall additionally, if requested by POL, provide the Termination Services. To request the Termination Services, POL must give CC a Termination Assistance Notice by no later than 29 December 2020 (4 months prior to expiry (paragraph 2.3(c)(ii)(D), 2019 Letter of Extension)). Note that under Schedule 8.5, paragraph 6.9, the notice period for a Termination Assistance Notice is 3 months but this has been amended by the 2019 Letter of Extension. POL is not required to give notice for CC to continue to provide the Services during the TAP.

The Termination Assistance Notice shall specify: (i) the date from which Termination Services are required, which may be up to 12 months prior to expiry of the Agreement; (ii) the nature of the Termination Services required; and (iii) the period which it is anticipated that Termination Services will be required, which shall continue no longer than 24 months after the expiry date. However please note that POL has an option to extend the Termination Services for up to 6 months beyond that 24-month TAP period by giving CC no later than 20 Working Days prior to the date on which the provision of Termination Services is due to expire (Schedule 8.5, para 6.10). Paragraph 6.14 of Schedule 8.5 details the scope of Termination Services which are mainly to assist and support the transition.

POL00423571

POL may terminate the requirement for Termination Services by serving no less than 20 Working Days written notice upon CC. This shall not have the effect of reducing the maximum possible duration of the TAP being 24 months after expiry of the Term.

Changes to the Services and Termination Services:
Under the 2019 Letter of Extension, the Services and Termination Services provided according to Termination Assistance Notice may be amended using the Change Control Procedure during the TAP, including to extend or reduce any time periods for the provision of any such Service or Termination Service. POL's right to terminate the TAP early for convenience after expiry of the Agreement would not apply as the clause does not survive expiry of the EUC Agreement.

Exit Plan

CC is required to provide an initial Exit Plan within 3 months from the Effective Date then provide the final Exit Plan no less than 6 months prior to the expiry of the EUC Agreement.

CC must review the Exit Plan annually and prepare a revised Exit Plan to reflect the changes in the Services and submit it to POL. The parties must then agree the content together. There is no provision for POL to initiate a request for changes to an Exit Plan but practically speaking, POL may raise such request during the review process of an Exit Plan.

If the parties cannot agree the final Exit Plan within 14 days from CC's delivery of the final Exit Plan to POL then the matter will be escalated in accordance with Schedule 8.1 (Governance) to be resolved by both parties within 5 Working Days from the escalation before going through the Dispute Resolution Procedure (paragraph 6.8, Schedule 8.5). Until such dispute is resolved, the last approved version of the Exit Plan will apply.

Transition

The transition of the Services may be phased (paragraph 6.6, Schedule 8.5). If the transition is not completed during the TAP, POL may request in writing that CC continue to provide Termination Services and additional services, including that are same or similar to the Services, on a time and material basis using the Rate Card (subject to indexation) following the TAP and until the transition has been effected (paragraph 2.3(c)(iv), 2019 Letter of Extension). The notice period for such request is not specified.

Procurement risk note

Residual Procurement Risk
There is a residual procurement risk attached to the use of the TAP from the point at which it was introduced into the EUC Agreement at the Preferred Bidder stage of the procurement for the EUC Agreement because it did not form part of the dialogue with bidders. Legal advice was provided in relation to that risk at the point of approval of the EUC Agreement. This advice identified the risk as low as transition services over the TAP timescales are not unusual for a ICT contract of this type and because it was envisaged that, at the time of the use of the TAP, procurement(s) would be underway for replacement services and so interested bidders would be motivated not to challenge.

At this stage, this residual procurement risk still applies and the use of the TAP has the potential to highlight this procurement risk as we believe that the market

is aware that the contract is due to terminate at the end of April 2021 and therefore will become aware that additional transition services have been agreed.

The use of the Services during the TAP
The Services and the Termination Services are identified separately in Schedule 8.5 of the EUC Agreement. Paragraph 6.1 makes it clear that CC has to provide the Services during the TAP and that POL can choose what Termination Services it requires.

Given that the procurements for the replacement services will be underway by the time the TAP begins, POL may consider the provision of the Services during this time is enabling the transition. There could be an argument made that this is not the case unless the Termination Services are also being provided quite quickly into the TAP, but this is not necessarily supported by the wording of Schedule 8.5. For this reason the more quickly the re-procurements are carried out the lower this risk.

Mitigating factors
Despite the risks attached to the use of the TAP outlined above, we consider that there are several factors mitigating these risks of successful challenge so that they remain low.

Firstly, we understand that the bidders from the original procurement who are most likely to become aware that the TAP has been agreed post Preferred Bidder stage given their knowledge of contract during the process are potential bidders for the re-procurements and so they are less likely to be motivated to challenge at this stage.

Secondly, any challenge would be limited to a damages claim because both a declaration of ineffectiveness and a penalty will be time barred. Bringing a damages claim when the timescale of the alleged 'breach' is limited to a few months while a procurement process is completed is likely to be advised against by legal advisors to a potential challenger.

The value of the Services during the TAP is estimated to be £5 million, which added to the £66 million spend under the EUC to date, is well within the value of up to £300 million set out in the OJEU notice. The OJEU notice also sets out that transition services will be provided after the termination date.

Even if the TAP could not be used to provide the Services post termination, it is likely that the provision of the Services would fall under the ability to modify a contract under Regulation 72(1)(b) in any event. While we understand that CC would be unlikely to agree to such an extension on the same terms and therefore this way forward is not an option, it does assist with an assessment that the risk of successful challenge in a Court is low.

POL00423571

Procurement Risk Exception Form

1.Business area or Project Details					
Date Raised	**2/11/20**	**Business Area/Project**	**Finance**	**GE Member**	**Al Cameron**
Raised By	**Tom Lee**	**GE-1 Exception Owner**		**Value of Award**	**£1.5m**
				Total Value	**£2.7m**

2.Exception Details									
Exception Title	PwC External Audit contract not extended into 3rd year								
Exception Type (New/ Contract Extension)	**Extension**	**Exception Category**	Agreement on third year fees not reached so contract not extended. Others(please specify)		**Exception ID**	*To be provided by Procurement*			
Detail of contract being entered into / extended.	PwC act as POL's external auditor. The initial term expired on 1 October 2020.It can be compliantly extended for up to a further 2 years but hasn't as of yet as POL and PwC have not reached agreement on 3rd year fees.								
How long are you asking the business to tolerate /accept this risk? (duration)	*3 months*	***Start date***	*1/10/20*	***End Date(s)***	*24 Dec 2020*				
Why does this contract need to be entered into / extended now? **What is the reason for the urgency?**	PwC act as POL's external auditor. The initial term expired on 1st October 2020. However thus far POL and PwC have not been able to agree the fees for the third year and so no extension has yet been signed.								
Impact if Exception Declined	Extension to contract remains unsigned. Post office will be in a weaker position for negotiating fees for the next 2 years, which may total c. £1.5m +								
PCR Risk Mitigation	**Y**				**Regulation X Exemption N**				
PCR Risk Level *[shade as appropriate]*	**LOW**	**MEDIUM**	**HIGH**		**Legal Risk Note supplied**	**Y**			

3. What controls are in place, actions completed or work in progress to mitigate the risk?		
Control or Action detail	**Target Date**	**Action or Control Owner [business / procurement]**
Negotiations on fees are usual for this type of contract. PwC are putting their request for an increase in writing. There is a process to be followed in order to address their request. This can result in dispute resolution if the 2 parties are unable to reach agreement on their own. However, it is hoped that a negotiated agreement will be reached as has happened in the past.	4/12/20	Finance
If no mitigation activities are feasible, insert an end date 6 months after contract award or 6 years if the award is not to be notified to the market.		

POL00423571

Procurement Risk Exception Form

1.Business area or Project Details					
Date Raised	**03/11/2020**	**Business Area/Project**	**Supply Chain**	**GE Member**	**Jeff Smyth**
Raised By	**Angus McDonald**	**GE-1 Exception Owner**	Gary Walker-IT Russell Hancock-Supply Chain	**Value of Award**	**£176,000**
				Total Value	**£1,236,339.96 since 2015**

2.Exception Details					
Exception Title	Award of further extension to Swindon stocks WMD (WCS) support and maintenance contract				
Exception Type (New/ Contract Extension)	**Extension**	**Exception Category**	Regulation Breach	**Exception ID**	*To be provided by Procurement*
Detail of contract being entered into / extended.	**Blue Yonder (formerly JDA Software Group) is an American software and consultancy company that has ended up owning and delivering support to POL of a bespoke version of the WMD (Warehouse Management Dispatcher).** **Blue Yonder having initially agreed to work through a compliant IT Reseller Framework in June of this year to bring the contract under compliance have reneged and refused to operate in such a way this week (WC 2/11). The company have only elaborated that they are not set up to work through resellers in this way and are not willing to invest time or effort in an approach to payments that they will not use elsewhere. We still have a need for the services, the renewal is shortly due, hence this PREN-there are no other avenues to achieve compliance.** ***Context:*** *"Swindon Stocks" comprises a series of legacy IT systems focused around Galaxy* *The Galaxy system acts as the main hub for the stock control system and holds master data for all products and address details for Branch, Royal Mail, Parcel Force and third parties.* *In relation to products, Galaxy stores approximately 11,000 products 30% of which are active at any given time.* • *Holds a large variety of master data about items, delivery sites and supplier contracts* • *Keeps track of stock availability* • *Takes in orders from POL branches and other warehouse client sites* • *Reserves stock, if available* • *Consolidates orders per delivery address and Passes orders to WCS for picking, packing and dispatch* • *Case management for customer queries* • *Provides our back office financial systems with data so that clients can be billed.*				

POL00423571

Procurement Risk Exception Form

	Galaxy receives orders from branches, as well as Royal Mail and Parcel Force depots, and fulfils them by interfacing with WCS and Mercia; note that it has both POL and RMG users. *Galaxy acts as a hub, with WCS (aka WMD), Mercia, POLSAP, Royal Mail and Parcel Force systems as spokes. A number of Access databases are used in conjunction with Galaxy, assisting in the management of master data, and the formatting of branch and client orders, all arriving from a variety of sources.* ***All of the other components have confirmed and compliant procurement routes for their renewals in March 2021.*** ***How does this product fit in?*** JDA (now Blue Yonder) provide software that is used within the Swindon supply chain stock centre to control the pick and pack/conveyor belt – "Warehouse Control System" also known by the vendor as "Warehouse Management Dispatcher". The contract was a CSC (now part of DXC) sub-contract, accessed via Royal Mail. The Deed of termination enabled POL to take a direct relationship with JDA to achieve separation from Royal Mail along with other software and systems components at Swindon this was compliantly done in 2015. In 2016 when the Back Office IT contract was being let all of the Swindon systems and support contracts were to be included however, they were descoped pending a further strategic review of the future of Swindon, the systems in operation and the potential to modernise or remove what was currently in operation. Board will be aware this has been an extended discussion and until this year the licenses/maintenance and support arrangements at Swindon have been renewed annually with a supporting risk note. **What Services are currently provided** **Software provision (JDA Warehouse Management Dispatcher), and support/maintenance for stock management systems located in Swindon. Custom reporting** **Current management arrangements** **Updates to supported software. Solution line telephone support / email support, option to migrate supported software to other operating platforms .**				
How long are you asking the business to tolerate /accept this risk? (duration)	1 year	**Start date**	15/11/2020	**End Date(s)**	15/12/2020
Why does this contract need to be entered into / extended now? **What is the reason for the urgency?**	The maintenance renewal dqte was the 10/11/2020, Blue Yonder the supplier of maintenance and support services have disengaged from the resale process and refused to accept any flow through terms or undergo any form of setup with a reseller. They have agreed to delay the renewal date in light of this to enable POL to finalise governance by four weeks				
Impact if Exception Declined	**The tool is not supported, operations at Swindon may be effected and the operation of other systems used for the management of stock and orders**				

POL00423571

Procurement Risk Exception Form

PCR Risk Mitigation	Y/N			Regulation X Exemption	
PCR Risk Level *[shade as appropriate]*	LOW	MEDIUM	HIGH	Legal Risk Note supplied	Y

3. What controls are in place, actions completed or work in progress to mitigate the risk?		
Control or Action detail	**Target Date**	**Action or Control Owner [business / procurement]**
If no mitigation activities are feasible, insert an end date 6 months after contract award or 6 years if the award is not to be notified to the market.		

POL00423571

Risk Note

Author: Ravi Mudundi Date: 04 Nov. 20

Risk Report

This is a Legal risk report prepared in respect of an agreement to provide software that is used within the Swindon supply chain stock centre to control the pick and pack/conveyor belt – "Warehouse Control System" ("Agreement") between Post Office Limited ("POL") and ("Blue Yonder").

Background and Purpose

I understand the Agreement was compliantly sourced in 2015.
Blue Yonder provides a software (JDA Warehouse Management Dispatcher), and support/maintenance for stock management systems located in Swindon ("Services")

The Agreement is due to expire on 15th November 2020 and POL has secured the Services beyond the expiry of the Agreement, via a reseller under the Health Trust Europe (HTE) Framework Agreement. POL appointed SCC as its reseller under the HTE Framework Agreement. POL has carried out this exercise in order to compliantly source the Services.

Whilst Blue Yonder were originally keen to provide the Services via SCC, they are now refusing to do so on the basis that they are not set up to work through resellers. POL is still engaging with Blue Yonder to enter into the arrangement. If Blue Yonder refuses to enter into an agreement via the reseller, then POL will have to renew the Agreement non-compliantly with Blue Yonder for continuation of the Services.

The purpose of this risk report is to summarise the key risks to POL if the Agreement is non-compliantly extended and the mitigating factors assigned to such risk.

CONFIDENTIAL AND LEGALLY PRIVILEGED. DO NOT FORWARD, SCAN, DISCLOSE OR COPY.

POL00423571

CONFIDENTIAL AND LEGALLY PRIVILEGED. DO NOT FORWARD, SCAN, DISCLOSE OR COPY

Appendix 1: Legal Risks – Privileged

The table below sets out the Legal Risks in more detail:

Risk	Mitigation	Probability[1]	Impact[2]	Overall Residual Risk
Public Contracts Regulations 2015 (PCR) The Services under the Agreement are subject to PCR and therefore must be competitively procured. POL has exhausted all options to extend the contract and therefore any further extensions are deemed to be non-compliant under PCR. There is a risk of challenge by other providers who provide similar services on the basis that they were not afforded the opportunity to bid for the contract as the services were not procured compliantly. The risk of any such challenge under the PCR appears to be low as I am advised that only Blue Yonder can support and maintain the Software as they own the	The Agreement should not be extended for more than a year and ensure that a plan is in place to re-procure the Services before the expiry of the contract. An extension for a short period is unlikely to attract attention from the market.			Medium Risk

[1] *Assessed after Mitigation taken into account*
[2] *Assessed after Mitigation taken into account*

CONFIDENTIAL AND LEGALLY PRIVILEGED. DO NOT FORWARD, SCAN, DISCLOSE OR COPY.

POL00423571

CONFIDENTIAL AND LEGALLY PRIVILEGED. DO NOT FORWARD, SCAN, DISCLOSE OR COPY

IPR and there are no suppliers in the market who provide support on the software. While the practical likelihood of a third party bringing a claim is low, if a challenge is indeed brought, such a claim is likely to be successful. Should a challenge be successful, this could lead to damages being awarded to them and the court could also direct the contract to be terminated.				

CONFIDENTIAL AND LEGALLY PRIVILEGED. DO NOT FORWARD, SCAN, DISCL

POL00423571

POST OFFICE LIMITED
GROUP EXECUTIVE REPORT

Title:	Barclays Bulk Cheque Processing Contract Extension - confirm the approach
Meeting Date:	11/11/20
Author:	Greg Lewis, Senior Commercial & Product Manager, Partner Banking, Martin Kearsley Banking Director
Sponsor:	Owen Woodley, Group Chief Commercial Officer

Input Sought

Action Required: Decision	The Group Executive is asked to **approve** the approach by the Banking team in relation to assessing what cheque processing option should be procured and the proposed next steps The Plan is to • Complete an RFI to gain greater market insight and validate supplier costs to build a business case • Return to the GE with a recommendation on what to procure along with the business case • Gain agreement to the extension of the contract for bulk cheque processing to allow time to procure the replacement contract (e.g. building, testing and integrating the solution).
Previous Governance Oversight:	A risk exception was approved by the Board in June 2020 to extend our cheque processing services for 1 year until 30 June 2021.

Executive Summary

Context:	Barclays provide cheque processing services for the out-clearing of Personal and Business cheques that we accept as a Method of Payment (MOP) at our Horizon Counters. This includes Banking Framework processing services for Cheque Encashment and Partner Bank Cheque Deposit Envelopes which we are committed to providing until the end of Banking Framework 2, that is the end December 2022. These services commenced in 2011 under an OJEU Tender Award, with the OJEU Notice stating a total contract duration of 8 or more years. However, the contract awarded was on a 5+3 basis. Approval was granted in 2018 to extend our cheque processing services for 2 years beyond the contracted term with Barclays until 30 June 2020.

POL00423571

	The contract was extended again last summer to 30 June 2021. The Banking Team now own this contract under the recent organisational review and are evaluating future service options, to move away from high-cost paper-based services using RMG and other couriers. Cheque scanning at the counter to improve the service offer to customers and remove the expensive costs of moving cheques to a central processor is the most likely outcome of this review. Consequently, a project to build a business case for cheque scanning at the counter is underway, including running an RFI to help validate the supplier costs. The plan is to start procurement in the new year subject to approval of this business case and funding.

POL00423571

Questions asked & addressed

1. What contracted services are being extended and why
2. What is the background to this request?
3. What options were considered?
4. What is required to re-procure these services?

Report

What contracted services will need to be extended and why?

5. Cheque transactions support core services such as Mails (stamps and parcels); Bill Payments (e.g., utilities); and PO Money Savings/ISAs. In 2019/20, a total of c1.9m cheques and c8.4m Partner Bank Envelopes were processed, at an OPEX cost of c£1.2m. By not continuing the current service with Barclays, it would result in cheques not being accepted across our branch counters as a method of payment and breach our contractual commitment on cheque deposit service with Banks. This would impact our credibility with customers, require contract changes with our partners who accept cheques for their services (e.g. DVLA, Bill Payments etc) and our ability to negotiate Banking Framework 3. We are committed under Banking Framework 2 to keep the deposit service until December 2022.

What other options have been considered?

6. An OJEU procurement process could be prepared and launched for a replacement AS IS service, however the current service loses c£3m p.a. mainly due to the Royal Mail overnight pouch service (c£4.4. p.a.) and a minimum term of 2-3 years would have to be offered to the market in order to make it attractive to bid. Hence, there is a wish to explore other commercial options via an RFI which was issued to the market in on 4/11/20. This will provide key market information that will mean we are better informed on what cheque processing option to procure (e.g., costs, solution risks and delivery timescales).

7. In parallel we are also exploring the opportunities to include the Camelot/Postal Order Corporate Banking contract which could help save on procurement, business and contract management resource if one supplier can provide both services.

Banking Framework 3 will provide the opportunity to either significantly increase the 'as is' cheque deposit service price to banks, possibly increased further with the offer of processing from a central point into clearing on banks' behalf (as we do with our MOP cheques), or offer an in-branch scanning solution if the RFI and resulting business case justify such investment, in particular that the cost base can be moved to a predominantly variable basis given the likely fall off in cheque volumes.

POL00423571

Financial Impact

The bulk checkout processing services are budgeted with 2020/21 OPEX forecasts at a full year cost of c£1.1m. The Royal Mail Pouch service currently costs c£4.4m p.a. This service was benchmarked in 2018 and there was insufficient geographical coverage with another vendor to deliver against the overnight SLA's agreed within Banking Framework 2.

Risk Assessment, Mitigations & Legal Implications

The assessment of risks, mitigations and legal implications is provided in the table below:

Risk / Legal Implication	Mitigation / Control
Discrepancies between original OJEU notice (8 or more years) and executed contract term (9 years to date), totalling 10 years, with the further 12-month extension, leading to possible procurement challenge for the extension periods beyond the advertised OJEU.	Publish an OJEU update of the Barclays extension as per external legal procurement advice from Stephenson Harwood LLP (SH) and Ashfords. Commence compliant re-procurement via the most optimal path once internal and external procurement, legal advice has been provided by Ashfords and assessed internally by all appropriate stakeholders.

Stakeholder Implications

8. The recommended approach outlined in this report is designed to minimise any impact to stakeholders, with the contract extension providing continuity to support the existing cheque transaction processing services. This will allow sufficient time for the business to explore the optimal cheque clearing solution now that the entire industry has recently completed the FCM industry programme.

Other Options Considered

9. We considered procuring the as-is service only, however we wish to explore alternatives via a RFI as well as establishing realistic timescales for introducing any new solution so it can be factored into the negotiations of new Banking Services (Banking Framework 3).

Next Steps & Timelines

POL00423571

15. The steps required to progress are provided in the table below:

Step	Description	Timeline
1.	**GE Approval** to continue the RFI and return in January with a decision on what services will be procured and how long the Barclays contract will need to be extended for.	13/11/2020
2.	**Board Approval** will be requested (if necessary) to agree the approach and timeline	tbc
3.	**GE Approval** on suggested cheque clearing solution to be procured and Barclays Contract extension	15/01/21
4.	**Board Approval** on suggested cheque clearing solution to be procured and Barclays Contract extension – Owen Woodley to sign off final terms	31/01/21
5.	**Contract Extension/Amendment** will be executed with Barclays subject approvals.	28/02/2021
6.	**Contract Award Notice** published to inform the market of Barclays contract extension	1/03/2021
7.	**Issue OJEU NOTICE to procure for cheque processing supplier –** Publish tender for replacement to Barclays contract	March 2021

Appendix A

Legal Risk Note.

POL00423571

CONFIDENTIAL AND LEGALLY PRIVILEGED

Risk Note

Author: Lucy Woods (Procurement) - Ashfords LLP Date: 23 June 2020

Summary

Post Office Limited ("**POL**") is seeking procurement advice in relation to a 12 month extension to its cheque clearing services.

POL can seek to use the exemptions in Regulation 72 of the PCR 2015 and the risk of such exemptions being effective if challenged in Court is **medium,** but that when assessed against the actual likelihood of challenge we consider this risk is **low**.

POL can further mitigate these risks of challenge by ensuring it publishes the required notices in the OJEU.

Background

Post Office Limited (**"POL"**) and Barclays Banks Plc (**"Barclays"**) entered into an agreement dated 7 May 2010 for the provision of cheque processing and related services (the **"Bulk Clearing Contract"**). We understand that the Bulk Clearing Contract originally had a maximum overall contract term of 8 years; an estimated value of £10 million; and was procured in accordance with the Public Contracts Regulations 2006, now replaced with the Public Contracts Regulations 2015 (the **"PCR 2015"**). The OJEU notice referred to a term of 5 years with an option to extend 'for three years or more'.

The Bulk Clearing Contract was amended:

- on or around 28 September 2016, to extend the initial term to 31 October 2016;
- on 25 November 2016, to amend and restate the contract. The amendments included an extension of the contract term to 31 July 2017; and
- in 2017 by a Deed of Variation to provide for an extension of the contact term until 30 June 2018, along with an additional right for POL to extend to 30 June 2020. As part of this Deed of Variation, the parties also agreed some commercial changes to the contract.

POL is now looking to agree with Barclays a further 12 month extension to the Bulk Clearing Contract, which would extend the contract to 30 June 2021 (the **"BCC DoV"**). Such extension also provides for some further amendments to the contract terms, including some amendments to liability for POL and Barclays and some review to the charges over the extension term. POL would like advice on the procurement compliance of the BCC DoV.

Behind the Deed of Variation there has been a complex background of the introduction of the image clearing requirements in the industry (the **"Image Clearing Obligation"**). We understand POL has continually reviewed the need to re-procure these services on the open market, however the implementation of the Image Clearing Obligation has caused significant delays to POL's ability to do that in a manner which does not affect services and is value for money. Originally due to be completed in 2017, the Image Clearing Obligation has seen the market struggle to meet the new obligations and as recently as early 2020 the market has only just settled to a point where POL could look to start a procurement with a sensible outcome.

POL00423571

Modification

The BCC DoV can be compliantly entered into provided that one of the exemptions set out in Regulation 72 of the PCR 2015 applies because the changes to the Bulk Clearing Contract represent a modification during its term. If one of the exemptions under Regulation 72 cannot be used then the BCC DoV could be held to be an illegal direct award.

There are two exemptions we consider may apply to the BCC DoV, that under Regulation 72 (1) (b) and that under Regulation 72 (1) (c).

Regulation 72 (1) (b) allows for changes to the Bulk Clearing Contract to add additional services provided that a change in contractor cannot be made because:

(a) of economic or technical reasons; and
(b) this would cause significant inconvenience or substantial duplication of costs.

We consider it is very likely that the Image Clearing Obligation had an effect which required the Bulk Clearing Contract to be extended past its original 8 year term using this exemption, however the Court would decide on the facts whether that was the case.

To be able to use this exemption, the total value of the services following the BCC DoV must not exceed £15 million. It is our understanding that the estimate total spend across the services to include the 12 month extension of the BCC DoV is £11.5 million.

Our concern about the use of this exemption is that it relates to the 'addition of services' and not changes to the contractual relationship generally. We understand that there have been various amendments to the commercial positions between POL and Barclays during the term (including SLAs historically) and the BCC DoV provides for both changes to the indemnity and liabilities of POL and Barclays and the charges for the services. Accordingly there is a risk that these changes are not purely the 'addition of services'. To the extend POL is comfortable that these changes are absolutely necessary due to the addition of the services for the increased term (and not due to the changing commercial circumstances of the parties) then we consider this exemption could be used. If POL is not confident in this position it can consider the use of Regulation 72 (1) (c).

Regulation 72 (1) (c) can be used by POL for the BCC DoV where POL can demonstrate that the changes have 'been brought about by circumstances that a diligent contracting authority could not have foreseen'. The benefit of this exemption is that it relates to all changes and therefore can include commercial changes as well as the addition of services provided that the changes do not change the overall nature of the contract. Again there would be a financial limit of £15 million for the use of this exemption.

In our view POL may find it harder to use this exemption given that the Image Clearing Obligation has been in place since 2017 and so lack of foresight is more difficult to demonstrate at this stage, however, it may be that the difficulties that the market would face with the Image Clearing Obligation over the last 3 years could not have been foreseen. Again, this would be for the Court to decide on the facts but we anticipate POL could put forward quite compelling evidence on this front having, as we understand it, looked to re-procure several times but considering that the market was not ready to be able to bid effectively.

The use of either exemption requires POL to publish a Modification Notice in the OJEU. We note this was not done at the last extension which increases the risk of challenge and

therefore we advise that this should be done this time to fully mitigate this risk (see section on mitigation below). For the BCC DoV we consider the risk of not being able to use the Regulation 72 exemptions as **medium** (but see below).

Consequences of an illegal direct award and likelihood of challenge

In the event it was held that the entry into the BCC DoV was an illegal direct award the consequences of such a finding are:

a) a declaration of ineffectiveness which would bring the contracts to an end with associated penalties; and/or
b) the award of damages by POL to the successful challenger.

To understand the likelihood of a challenge arising we need to consider the potential challengers, which are those providers on the market who provide cheque clearing services. A risk only crystallises if a challenge is brought.

Our understanding from POL is that the market has not been in a position to effectively bid for these services if they had gone out to market at any point between 2017 and early 2020. To the extent this is correct then we can assume that the likelihood of a market player wanting to bring a challenge is greatly reduced. POL needs to ensure that its procurement strategy from early 2020 onwards allows for the services to be re-procured in the most efficient way possible on the basis that the extensions are only being put in place to cover the gap between the Image Clearing Obligations settling down to a point where the market would be able to effectively bid and when a procurement could be completed.

This assumption is supported by the fact that any market player who was interested in the services would have been aware that the BCC Contract was due to end in 2018 according to the OJEU notice and therefore POL may have expected a challenge before now, if there was an appetite for a challenge on the market.

For this reason we would assess the actual likelihood of successful challenge as lower than set out earlier in this note and would therefore consider it to be **low**.

Mitigations

By publishing notices in the OJEU in relation to the use of the exemptions set out above, POL will be doing what it can to 'notify' the market and seek to set the time limit for challenges running.

POL must balance this against the risk of highlighting the presence to the market of the DoV however we would assume that the nature of the market is such that POL's relationship with Barclays is already well known.

For a claim for damages a challenger would have 30 days to raise a challenge from the date they knew or ought to have known about the DoV. This time limit can be extended by the Courts by up to 3 months where there is 'good reason' for doing so. Publishing notices in the OJEU of the change will assist with an argument that the 30 days runs from the date of that publication, although this will ultimately be determined by the Court.

For a claim for a declaration of ineffectiveness no challenge could be brought after a date falling 6 months after the DoV was entered into.

POL00423571

Procurement Risk Exception Form

1.Business area or Project Details					
Date Raised	**19/06/2020**	**Business Area/Project**	**Payment Acceptance | Commercial/Barclays Cheque Contract Extension**	**GE Member**	**Owen Woodley**
Raised By	**Nick Spicer**	**GE-1 Exception Owner**	**Andrew Goddard**	**Value of Award**	**c.£1.1m**
				Total Value	**c£11.5m**

2.Exception Details					
Exception Title	*Barclays Cheque Processing "Bulk" Contract Extension to 30/06/2021.*				
Exception Type (New/ Contract Extension)	**Extension**	**Exception Category**	Others(please specify)	**Exception ID**	*PREN18*
Detail of contract being entered into / extended.	*Barclays provide cheque processing services for the out-clearing of Personal and Business cheques that we accept as a Method of Payment (MOP) at our Horizon Counters. This includes Banking Framework processing services for Cheque Encashment and Partner Bank Cheque Deposit Envelopes. These services commenced in 2011 under an OJEU Tender Award, with the OJEU Notice stating contract duration of 8 or more years. The contract has been extended to 30 June 2020 with internal and external legal procurement advice sought, including external legal counsel Stephenson Harwood. Additional legal advice has been sought and obtained from external legal counsel (Ashfords) in June 2020 which is attached.*				
How long are you asking the business to tolerate /accept this risk? (duration)	*12 months*	**Start date**	01/07/2020	**End Date(s)**	30/06/2021
Why does this contract need to be entered into / extended now? **What is the reason for the urgency?**	In 2015 POL initiated a programme to meet the industry wide HMT and Cheque & Credit Clearing Company (C&CCC) directive to transition from physical paper to image clearing in 2017. Subsequently, the industry wide programme suffered significant issues and as a consequence the full migration from paper to image clearing was delayed to Q4 2019. We have received an initial recourse of £333k from Barclays for the issues and delays and they have remediated to point of stability in Q2 2020. Approval is now sought to extend the services for a further 12 months in order to re-procure these services during this further 12 month extension to 30 June 2021.				
Impact if Exception Declined	Cheque transactions support core services such as mails (stamps and parcels); Bill Payments (e.g. utilities); and PO Money Savings/ISAs could not be processed, resulting in cheques not being accepted across our branch counters as payment. This would impact circa £0.7 billion of our turnover per annum [current annual value of cheque payments].				
PCR Risk Mitigation	**Y**			**Regulation / No PCR compliant exemption**	
PCR Risk Level *[shade as appropriate]*	**LOW**	**MEDIUM**	**HIGH**	**Legal Risk Note supplied**	**Y**

PREN18

POL00423571

Procurement Risk Exception Form

3. What controls are in place, actions completed or work in progress to mitigate the risk?		
Control or Action detail	**Target Date**	**Action or Control Owner [business / procurement]**
Take external legal advice by publishing an OJEU update.	**Complete by H1 2020 (calendar year)**	**Antony Ray/ Nick Spicer**
Simplify the services by removing the majority of POL specific requirements by adopting the Standard Image Clearing Switch File and Message formats, processes and policies. This will reduce the cost upfront and ongoing as well as the procurement and implementation timescales (if we were to award to an alternate supplier to Barclays).	**Already Completed in H2 2019 (calendar year)**	**Nick Spicer/ Caitlin Lloyd (and Cheque Image clearing Programme Team)**
Drafted contract extension amendment and reinstatement in conjunction with Barclays, incorporating the new standard Industry Image Clearing Standards.	**Draft completed H1 2020.**	**Nick Spicer/ Antony Ray/ Caitlin Lloyd/ Renata Prywerek/ Ravi Mudundi**
Re-procurement of the services under either one of two CCS Framework Agreements that Ashfords are currently reviewing, or in the event these frameworks do not meet the technical and business requirements, the alternative is to carry out a full OJEU tender. However, due to the interdependencies and connected nature of this contract to the separate Barclays Corporate services agreement and Barclays Postal Orders and Camelot Cheque Contract, we have an option to carry out as a single OJEU tender.	**H2 2020** **(Activities: Review 2x CCS frameworks against new simplified requirement under Image Clearing to be completed by end of 2020 calendar year).**	**Nick Spicer/ Caitlin Lloyd/ Antony Ray/ Ravi Mudundi/ Renata Prywerek**

PREN18

POL00423571

18.1

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	12th November 2020
Author:	Reena Chohan, People and Policy Compliance Manager	**Sponsor:**	Jonathan Hill, Director of Compliance/Ben Foat, Group General Counsel

Input Sought: Discussion & Approval

The Committee is asked to review and approve the updated policies and endorse the proposed actions for the business for onward submission to the Audit, Risk & Compliance Committee (ARC).

Please note that the current proposal from the Chair of the ARC is that approval of the below policies will be via written resolution before the ARC meeting to free up time on the main ARC agenda.

Executive Summary

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

Questions addressed in this paper

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

Which policies were updated in this annual cycle review?

1. In this review cycle the following **5** policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Owner	Governance Approval Body
Change Management Policy	Nov 2019	Minor updates, using revised template and to include new personnel.	Dan Zinner	RCC & ARC
Conflicts of Interest Policy	May 2019	Legislative review	Ben Foat	RCC & ARC
Risk Policy	Nov 2019	**Risk policy is be discussed separately in Mark Baldock's risk update paper**	Alistair Cameron	RCC & ARC

Confidential

POL00423571

Risk Appetite Statement	May 2016	**Risk Appetite is be covered separately in Mark Baldock's risk update paper**	Alistair Cameron	RCC & ARC
Freedom of Information Policy	New Policy	This is a new policy that LCG are proposing Post Office adopt	Ben Foat	RCC & ARC

What updates were included and why?

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

Change Management Policy:

In this annual review there were minor updates, this included using the revised template for the policy to be updated on, along with details of new personnel.

Policy Compliance View

This policy was significantly updated last year. The policy directs clearly what constitutes a change, how changes should progress through governance and the change principles which balance these aspects and seek to reduce the risks associated with change.

The Change Excellence Framework SharePoint site provides detailed oversight of all the processes and controls in place.

The Strategic Portfolio Office also ensures that training is provided for all Heads of Transformation Portfolio and Change resources, covering any changes to governance processes. Any new resources are provided with more in-depth training to ensure their understanding and compliance to the standards.

Conflicts of Interest Policy:

This has had a thorough reviewing covering the below additions:

1.3 - Inclusion of definition of a person connected with a director;

1.6. - Improved detail on directors' duties under CA 2006 and compliance with the UK Corporate Governance Code;

2.4 - New reference to the Post Office Conduct Code relating to business standards and greater detail on the process for reporting.

2.4 – Procurement; new section on managing procurement conflicts, signposting the existing declaration process.

2.4 – Directors; new section on considerations for directors when identifying and reporting actual or potential, direct or indirect interests.

Policy Compliance view

A comprehensive update- we have agreed to explore with Co Sec areas to test for control gaps as part of our second line compliance review.

POL00423571

Protecting Personal Data Policy:

No substantive changes, minor updates to section 1.7 to add Freedom of Information Act, 3.1 to include the eCase tool and 4.3 to refer employees to the Data Protection intranet page for further help.

Policy Compliance View

Control Standards can be demonstrated as being met; however, these do require the action and support of Data Owners within the business to ensure these are effective controls. The working Personal Data Incident, Breach Management and Post Office Individual Rights Procedures, demonstrate the controls in place and the minimum control standards stated are being met.

Risk Policy:

The Risk Policy and Risk Appetite Statement are to be covered separately in Mark Baldock's risk update paper.

Policy Compliance View

Each minimum control standard stated within the Policy is currently operating. Evidence of each control is either reflected in the corporate GRC tool or maintained by Central Risk who own the risk registers, compliance with the policy is demonstrated through the Risk Registers which provide a detailed oversight of all the processes and controls in place.

Freedom of Information Policy:

This is a new policy that LCG are proposing Post Office adopt.

Policy Compliance View

Given that this is an introduction of a new policy the attestation on the policy performance will need to be made and carried out next policy annual review.

Assurance

Working with policy owners we are piloting the assurance process and sample testing policies on a risk basis to review the policy standard and policy compliance.

The Key Policies Intranet Page has now been updated and reflects the following:

- Policy cycle document to show when policies were last reviewed and are due for their next review;
- Policy Approval Form;
- All Group Key Policies.

The page is still work in progress with more content to be added as compliance continue to develop and build a governance framework around our policies.

POL00423571

Conclusion

We continue to work with Policy Owners and Company Secretariat to ensure we maintain our policy governance responsibilities and undertake assurance that the polices are working as expected. This is a key part of the wider Post Office controls work.

POL00423571

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

19

Title:	Directors & Officers (D&O) Insurance Renewal	**Meeting Date:**	12 November 2020
Author:	Edward Dyer, Working Capital and Cash Management Lead	**Sponsor:**	Alisdair Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to note the details of the insurance renewal for 2020/21 and particularly the Directors & Officers Insurance Renewal..

Executive Summary

Post Office's insurance cover has been renewed in line with the Audit, Risk & Compliance Committee (ARC) paper dated 28 October 2020 at a total cost, in line with the estimate presented, of £2.1m.

Following the ARC approval, the Crime insurance deductible was increased from £2m to £6m and the corresponding guarantee from NatWest in favour of the Bank of England was raised accordingly. A breakdown of the insurance premiums is presented in Schedule 1.

Report

D&O Insurance Renewal Challenges

D&O Market Contraction

1. The following factors have driven significant price increases in the D&O insurance market:
   - Declining value of insurer investments (insurers invest premiums before having to pay out for claims);
   - Increased claims (Lloyds H1 predicted profits of $1.25bn deteriorated into a $0.5bn loss. Lloyds ultimately expects to pay Covid-19 claims of over $4bn);
   - Lower premium volumes (from reduced economic activity);
   - The impact of the virus to the global insurance industry is estimated at over $200bn, half of which is reduction in insurer investment values; and
   - The potential for D&O claims arising out of (Covid-19 related) insolvencies in 2020/21 is of serious concern to insurers.

2. As a result of these issues, market capacity has reduced, driven by some insurers exiting D&O insurance and others taking more cautious, reduced positions.

3. Post Office Limited's (POL) pricing was also impacted by:
   - Horizon liabilities; and
   - Lack of appetite from some insurers for financial institutions exposure (Lockton explained to insurers that we are not a bank but provide banking services).

4. Schedule 2 sets out the experience of other corporates. For example, one retailer experienced a 10x increase in premiums for D&O cover of £40m compared to £60m

Strictly Confidential

POL00423571

the previous year. Lockton noted that those companies with higher D&O insurance cover than POL's £60m typically have operations in the USA.

5. POL's £60m D&O policy has been renewed at a cost of £292,000, a 160% increase on the 2019/20 premium of £112,500.

Why did the renewal run late?

6. On the 1 November 2020 renewal date, £40m out of the £60m of cover was in place. By 5 November this was made whole with £20m of additional cover backdated to the renewal date.

7. The delay was caused by market conditions whereby insurers introduced much more stringent processes to underwriting risks. Most renewals now require senior management sign-off and the interrogation of risk has become significantly more rigorous, resulting in greater work for underwriters and a subsequent slowing of renewal processes. Further, whilst renewal was initiated earlier than usual, insurers were unwilling to engage in meaningful discussions until close to renewal, as they dealt with renewals from the 30 September quarter date.

8. Historically, POL's insurers have not required updated financials prior to renewal, accepting receipt of these sometime after renewal. This year, late in the process, these became a 'must have' before some insurers would provide terms. Insurers paid much closer attention to the regulated and Financial Institutional aspects of the Post Office business and required a detailed update on the Horizon issues. This arduous process has not been unique to Post Office, however, and has been a challenge for brokers and their clients across the market.

Schedule 1: Insurance Premiums

Insurance Premiums - 2020/21 Renewal
(£ in millions)

	Premium 2019/20	Premium 2020/21	vs Last Year (£)	vs Last Year (%)	Comments
Crime*	786,672	930,000	143,328	*18%*	Deductible increase from £2m to £6m
Cyber	265,000	311,375	46,375	*18%*	
D&O*	112,500	292,000	179,500	*160%*	
Combined Liability	103,892	108,950	5,058	*5%*	Long-term Agreement
Motor	101,617	103,426	1,809	*2%*	Long-term Agreement
POL PI	91,250	127,750	36,500	*40%*	
POMS PI	75,000	92,500	17,500	*23%*	Cover increased from £5m to £10m
PDBI	72,668	85,000	12,332	*17%*	
Terrorism	16,250	16,250	0	*0%*	Long-term Agreement
PA Travel	14,950	12,500	(2,450)	*-16%*	
Special Contingency	0	14,500	14,500	*N/A*	3 year policy term. Pricing unchanged.
Total (with £6m Crime deductible)	**1,639,799**	**2,094,251**	**454,452**	***28%***	

All premiums exclude UK Insurance Premium Tax at 12%

POL00423571

Schedule 2: D&O market examples provided by Lockton

Sector	Limit at renewal	Outcome
Retail	£60m	Only £40m available; price increased 10x
Retail		Distressed risk; premium increased 15x for half previous limit
Real Estate	£100m	135% premium increase
Security	£100m	500% premium increase
Building materials	$65m	189% premium increase
Real Estate (private)	£10m	40% premium increase
Commodities (private)	£20m	132% premium increase

Strictly Confidential

POL00423571

20

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	24 November 2020
Time:	08:50 – 11.30
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Tom Lee (Head of Finance Financial Accounting and Controls)
Ken McCall (SID)	Mark Underwood (LCG Operations Director): Item 4
Tom Cooper (NED, UKGI)	Christine Kirby (Financial Controls Manager): item 6
Zarin Patel (NED)	Amanda Bowe (Post Office Insurance ARC Chair): Item 7
Regular Attendees:	Ed Dutton (Post Office Insurance Managing Director): Item 8
Tim Parker (Group Chairman, POL)	Nick McCowan (Post Office Insurance Head of General Insurance): Item 8
Nick Read (Group CEO)	Ian Holloway (Post Office Insurance Director of Risk & Compliance Director): Item 8
Alisdair Cameron (Group CFO)	Declan Salter (GLO Director): item 9
Ben Foat (Group General Counsel)	Graham Hemingway (Historical Matters Portfolio Lead): Item 9
Andrew Paynter (Audit Partner, PwC)	Andrew Goddard (Payzone MD): Item 10
Sarah Allen (Senior Manager, PwC)	Amanda Jones (Group Retail and Franchise Network Director, Interim): Item 11
Rachel Owens (Senior Manager – Digital Audit, PwC)	Karl Oliver (Head of Commercial Partnerships): Item 11
Johann Appel (Head of Internal Audit)	Dan Zinner (Group Chief Strategy and Transformation Officer): Item 12
Mark Baldock (Head of Risk)	Saira Burwood (Head of SPO): Item 12
Jonathan Hill (Compliance Director)	
Rebecca Whibley (Senior Assistant Company Secretary)	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: 690 753 133# Pin (if applicable): 58042	

Time		Item		Owner	Action
08:30 -08:50		Meeting with Auditors and ARC Committee without Management present		Auditors	Discussion
08:50	1.	Welcome & Conflicts of Interest		Chair	Noting
08:55	2.	Previous Meetings		Chair	Approval
		3.1	Minutes (22 September 2020)		
		3.2	Action List		
		3.3	Draft Risk and Compliance Committee Minutes (12 November 2020)		
09.00	3.	Risk, Compliance and Internal Audit Updates			
		3.1	Risk Update (Archer Dashboard)	Mark Baldock	Noting

DRAFT

Strictly Confidential

POL00423571

POST OFFICE LIMITED

		3.1.1	Risk Policy, including the proposed approach to Risk Appetite & Key Risk Indicators		Approval (onward submission to Board)
09:10		3.2	Compliance Update	Jonathan Hill	Noting
09:20		3.3	Internal Audit Update	Johann Appel	Noting
09:30	4.	Suspense Accounts		Mark Underwood	Noting & Approval
09:45	5.	Audit Plan 2020		Andrew Paynter	Noting
09:55	6.	Financial Reporting Council Framework Update		Tom Lee & Christine Kirby	Noting
10:05	7.	Update from Subsidiaries: verbal update from Post Office Management Services ARC		Amanda Bowe	Noting
10:20	8.	Financial Conduct Authority Dual Pricing Change		Ed Dutton, Nick McCown & Ian Holloway	Noting
10:30	9.	Historical Matters Unit (HMU) Governance Review		Declan Salter & Graham Hemingway	Discussion
10:45	10.	Payzone Risk Report		Andrew Goddard	Noting
11:00	11.	Deepdive: Multiple Partner Failure		Amanda Jones & Karl Oliver	Noting
11:15	12.	Deepdive: Transformation Office Change Update 2020		Dan Zinner & Saira Burwood	Noting
	13.	Any other business		All	Noting

Items for Noting

These items will not be presented to the Committee and any questions should be sent to the Secretary for submission to the author for response. Questions and answers will be recorded as appendices to the meeting minutes.

	1.	PCI-DSS and Cyber Security Update		Noting
		1.1	PCI-DSS	Jeff Smyth & Rob Wilkins
		1.2	Cyber Security	Tony Jowett
		1.3	Joiners, Movers, Leavers	Tony Jowett
		1.4	Belfast Datacenter (Horizon) DR Post Test Briefing	Gary Walker
	2.	Data Governance		Jonathan Hill & Ben Foat

DRAFT

Strictly Confidential

POL00423571

POST OFFICE LIMITED

	3.	Law & Trends Forum	Sarah Gray & Ben Foat	
	4.	Agreed Upon Procedures	Tom Lee, Brian Kelly & PWC	
	5.	Supplier Contracts Out of Governance	Barbara Brannon	

Items for approval via Written Resolution

These items will not be presented to the Committee and approval will be sought via Written Resolution to be signed by members prior to the meeting. Any questions relating to these items should be sent to the Secretary for submission to the author for response.

	1.	Policies for Approval:	Jonathan Hill	Approval
		1.1 Summary Paper		
		1.2 Change Management		
		1.3 Conflicts of Interest		
		1.4 Protecting Personal Data		
		1.5 Freedom of Information & Environmental Information Regulations		

Next ARC Meeting: Tuesday 26 January 2020 at 09.00 to 11.30 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ

DRAFT

Strictly Confidential