



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	
	Chrysanthi 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).	



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. 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.	



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.	

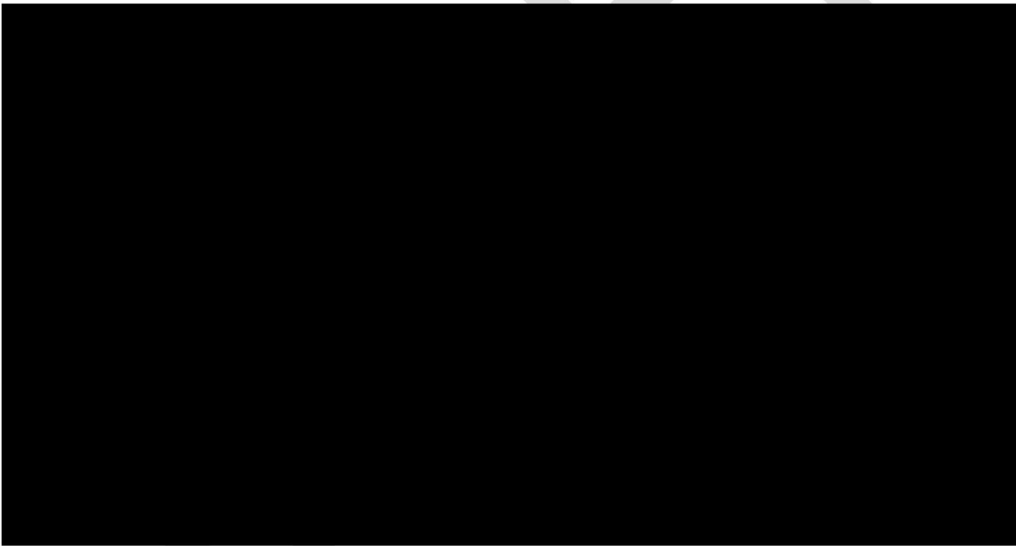


6.3	Although JS noted the slippage with the delivery of the payment solution, he remained confident all timelines and plans would be met on deadline. The Committee requested key milestones (including contractual milestones) be clearly highlighted in the paper for ARC. The PCI-DSS Programme Update was 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 i.e. 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 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 Locktons 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 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: •  •	
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	



	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.	



	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.	