POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance Committee ("RCC") meeting held via Microsoft Teams
on 13 July 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	
	Tony Jowett (TJ)	Chief Information Security Officer	Item 4
	Joseph Moussalli (JM)	Programme Manager, Project Managers and PMOs	Item 4
	Rob Wilkins (RW)	Cloud Services Director, MI, Data Strategy & Analytics	Item 4
	Tim Armit (TA)	Business Continuity Manager	Item 5
	Tim Perkins (TP)	Head of Security, Safety & Loss Prevention, Loss Prevention	Item 7
	Maxine Cross (MC)	Head of Reward & Pensions, Reward & Pensions	Item 8
	Sarah I Gray (SIG)	Group Legal Director	Item 9
	Andy Kingham (AK)	Head of Network, Retail Network	Item 10
	Sally Smith (SS)	Head of Financial Crime	Item 10
Apologies	Nick Read, Group CEO Owen Woodley, Group Chief Commercial Officer		

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 6 May 2020 were **APPROVED**.	
2.2	Progress on completion of actions as shown on the action log was **NOTED.** The following action updates were provided: - Action 3.3 from 6 May 2020 relating to COVID-19 wider enterprise risk statement had been discussed at June's GE and could therefore be **closed**. - Action 3.9 from 6 May 2020 relating to **Belfast Data Centre Exist and move to the Cloud** is being discussed at July's GE meeting and could therefore be **closed**. - Action 3.10 from 6 May 2020 relating to Whistleblowing can be **closed**. An update is being presented at this RCC meeting. - Action 3.15 from 6 May 2020 relating to the fit and proper policy would remain **open** until LC and JT had discussed HR involvement in the policy. - Action 3.15 from 6 May 2020 relating to Internal Audit Reviews could be **closed**. Updates have been provided to ARC. - Action 3.16 from 6 May 2020 relating to Status of Internal Audit actions could be **closed**. Updates have been provided to ARC and actions continue to be tracked. - Action 3.3 from 14 March 2020 related to an IA Cyber Security audit in FRES would remain **open**. No audit had been completed as yet. - Action 6.6 from 14 March 2020 related to Annual Legal Risk Report 2019/20 would remain **open**. The item has been added to the programme cycle for September and March.	**To do:** **LC/JT** **JA/TJ**

	- Action 10.6 from 14 January 2020 relating to supervisory HMRC meetings between BF and POL's new supervisor would remain **open** until the meeting had been completed. HMRC are not conducting meetings at present following COVID but SS would chase a meeting date. - Action 3.2 from 7 November 2019 relating to supplier contracts out of governance (SSK) remained **open**. Funding was on hold until October. - Action 5.3 from 7 November 2019 relating to a Cyber Security major incident test remained **open**. A test would still required. - All other recommended actions for closure were **closed**.	**SS** **JS/TJ**
3.	**Combined Risk, Compliance and Audit Update**	
	Risk	
3.1	MB presented the risk report. Focus since the last meeting had been on embedding the three lines of defence model into POL. Archer had been populated with 453 clearly identified risks and owners (15 overarching enterprise risks, 70 linked intermediate risks and 350 subsidiary local risks) and work has also been completed to assimilate the POL Covid-19 risk identification and management activity into the wider enterprise risk.	
3.2	Approval has been received from GE to refresh the corporate risk appetite statements (last reviewed in 2015) and to establish a supporting set of key risk indicators using existing KPI data. A pilot is underway to plot a set of KRIs for with Operations/Legal, IT and Finance.	
3.3	The Committee noted the following key enterprise risks remain: • 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. • Technology – POL is heavily reliant on key 3rd IT parties that is difficult to influence and has an ageing IT infrastructure. There is concern that the disaster recovery regime is ineffective. • Operational – low quality branch network locations and remuneration package for agents may impact revenue for POL and PostMasters. Change Portfolio remains at Amber.	
	Compliance	
3.4	JH presented the compliance report with the following points noted. **Telecoms**: JH noted that POL continues to prioritise fault repairs for vulnerable customers and to honour the commitments made to DCMS. Weekly updates continue to be requested by Ofcom who have now resumed their monitoring and enforcement programme. The Committee raised concern with POL's inability to effectively deal with S136 and 137 information requests, in terms of the accuracy of information provided to the regulator and the reliance on 3rd party providers for information without carrying out sufficient checks. The Chair requested that a comprehensive response programme be developed to reduce the possibility of being penalised.	**To do:** **TL/BF/JH**
3.5	**Fairness:** JH reported (Ofcom) would be reporting on fairness in early 2021 and that POL is considered (by the regulator) to have a high number of customers considered 'vulnerable' i.e. those who have been paying higher prices than customers in contract for more than 2-3 years. 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.	**Action** **MS**
3.6	**GLO/Freedom of Information Requests:** JH remarked resource has been stretched responding to Historic Shortfall Scheme, related/linked FOI requests (55 as at 24.06.2020) and CCRC requests. The	

	sensitivity/complex nature of the FOI requests has required external legal support, as well as approval from the GLO Steerco and notification to UKGI before release.	
3.5	**Belfast Data Centre Exist and move to the Cloud**: JH noted that data migration from the Belfast Data Centre is planned for eight weeks' time, and that an approach has been agreed between IT, Legal and Compliance. This approach enables POL to deploy a contractual and operational solution that eradicates the need for approval from upstream clients where personal data may be processed outside of the EEA. A compliant solution inside POL's Risk Appetite has been identified and is under development. JS noted that the talks with upstream clients and the short time from for data migration would be challenging.	
3.6	**Cookies**: JH advised a solution has been built and deployed to meet the Directive 2009/136/EC, (known as the Cookie Law), however the solution does not fully satisfy all regulator (ICO) consents. The Data Protection and legal teams are reviewing the implications to POL following a recent case in Germany where a company used a similar solution to POL's but was deemed to be non-compliant with EU legislation.	
3.7	**Financial Crime:** there has been a large increase in suspicious activities reports during lockdown, with 930 SARs and 159 investigations in April & May (cf 598 and 84 in April & May 2019). The team is working closely with the banks to understand the reasons for the spike.	
	Internal Audit	
3.8	JA presented the IA report. A summary of findings from last year's IA programme (2019/20) noted 171 audit actions across 25 audits in total (cf 271 actions across 24 audits in 2018/19). JA advised the lower number of actions could be attributed to a general improvement in the control environment. Some improvements are required in core controls following system and organisational changes during the year, risk management and governance oversight has slightly decreased, but information, communication and report turnaround has improved. JA was asked to consider ways of improving core controls.	**To do: JA**
3.9	The Committee noted the following audits have been completed since the last ARC meeting (6/5/20): • FS Branch Sales (FY20 IA Plan) (Final Report) • CV-19 Programme Assurance - Ph1 Set-up & Governance • Minimum Control Standards – Ph1 Cash Controls • Minimum Control Standards – Ph2 Minimum Control Standards – Ph2 • Cyber Security Maturity Assessment • Effectiveness of Second Line during CV-19 – Ph1. The combined Risk, Compliance and Audit paper was **NOTED for onward submission to the ARC.**	
4.	**PCI-DSS and Cyber Security Update**	
	PCI-DSS Programme Update	
4.1	JS presented the PCI-DSS update. He reported further funding has been agreed by the Board (26 May 2020 Board meeting) to progress the programme until completion, and that NR and JS had met with Paula Felstead, Ingenico Group CTO. Ingenico had provided a renewed commitment to achieve Vocalink Accreditation by the end of December 2020. The Banking forum has also been updated with a plan/timetable of key dates for 2021, indicating Pilot and Branch rollout commencing in February 2021. He expects formal PCI DSS accreditation to be achieved by June 2021.	
4.2	The following PCI key risks were discussed:	

	• Any additional essential changes required to the Fujitsu /Ingenico software would impact the planned timeline. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis there are no further changes. • Concern that POCa payments cannot be routed through Vocalink within the timescales. The team is working to identify a solution. • Concern that Santander cannot migrate payments to route through Vocalink within the timescales. The team is working closely with Santander.	
4.3	The Chair noted the progress made, but requested the report should clearly identify what progress has been made, the areas completed, those on track or not, and those that remain outstanding. Technical jargon should be avoided. The PCI-DSS Programme Update was **NOTED for onward submission to the ARC.**	
	Cyber Security	
4.4	TJ presented the Cyber Security update. **Cyber Security Maturity**: good progress has been made with the Deloitte cyber security maturity assessment and a report from Deloitte is expected in July detailing detailed actions for further mature Cyber controls. In the interim, Internal Audit has worked with Deloitte to provide an overarching report giving key recommendations and maturity assessments. Compared to last year, TJ believes maturity is more secure, and that focus should be on developing a cyber security strategy as the business and IT strategies unfold.	
4.5	**Covid-19:** TJ noted that during the pandemic, phishing traffic had increased but that SPAM-based mail attacks now appear to have returned to normal levels. The team has completed a targeted phishing simulation to raise awareness within POL.	
	Joiners Movers Leavers (JML)	
4.6	TJ presented the JML report. JML remains a key focus for the team. A draft reference model has been developed identifying the role and accountability of each department in the JML process, helping to reduce single points of failure. Good progress has been made enhancing the integrity of the links between Success Factors, Microsoft Identity Manager and Active Directory which controls access administration and the project is expected to be completed in August 2020.	
4.7	Regarding third party access to JML, although the team conducts audits, POL remains reliant upon suppliers being honest. A move to a cloud (such as Belfast Exit project) presents an opportunity for greater oversight and control.	
4.8	The Chair noted the progress made, but remarked ARC would question why the project had not been completed, as well as the lack of control over 3rd party access. The Cyber Security Update and JML report was **NOTED for onward submission to the ARC**.	
5.	**Business Continuity Update and Business Continuity Policy**	
5.1	TA presented the Business Continuity update. A complete failure of Horizon (no strategy has been developed for large scale failure) remains POL's key risk, but the current approach to resilience remains effective.	
5.2	Covid19 has demonstrated that POL can run effectively via home working for an unlimited period of time, and the ability to maintain call centres with home working including supporting a third party POCA call centre, means a solution is now being considered and explored. The 'Post Office on Wheels' (deployed for contingency purposes) has proved effective during the pandemic, however plans should be developed to mitigate against a second Covid wave.	
	Business Continuity Policy	
5.3	TA advised there have been no material changes to the policy since last year and that it remains suitable for purpose.	
5.4	The Business Continuity update and Policy were **NOTED for onward submission to the ARC.**	
6.	**GDPR Update**	
6.1	JH presented the GDPR update.	

	The team has now completed a review of contracts not previously remediated or de-scoped during the original GDPR remediation programme, identifying 7 key contracts as high risk including: • CWU • Unite • Fujitsu Telecoms • Global Payments • OH Assist • RAPP • Selenity.	
6.2	Work is underway to support the contract owners, however the Committee remains concerned that other high risk contracts may be identified following programme completion. The GDPR Update paper was **NOTED for onward submission to the ARC.**	
7.	**Suspense Accounts**	
7.1	[redacted]	
7.2	[redacted]	
7.3	[redacted]	**Action:** **TP**
7.4	The paper was **NOTED for onward submission to the ARC.**	
8.	**Pensions Assurance**	
8.1	MC presented the Pensions Assurance paper. She advised that ahead of the POL purchasing its share of the Royal Mail Pension, the project had identified a number of material systemic errors in the provision of pensionable data provided by POL to the Royal Mail Pensions Service Centre.	
8.2	These errors are predominantly linked to the incorrect configuration of Success Factors, and the misinterpretation of how promotional increases are treated in the pension terms. Willis Towers Watson (POL's actuarial advisers) has been engaged to help identify the extent of these errors, and to assist with mitigation to avoid future error. An internal audit has also been commissioned to understand why this has not been previously identified, and to ensure that any lessons are learnt.	
8.3	[redacted]	
8.4	The paper was **NOTED for onward submission to the ARC.**	
9.	**Law and Trends Update**	
9.1	SIG presented the Law and Trends update paper.	
9.2	She explained the purpose of the paper was to highlight any future legislation and or regulation that may impact POL, bringing the following to the Committee's attention: • Covid 19 Employment Legislation Updates. • ATM Additional Business Rates Update. • Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations.	

9.3	**Covid-19 Employment Legislation Updates**: there has been a recent flurry of legislative changes to react/mitigate against Covid-19. The Coronavirus Act 2020 (effective 25 March 2020) introduces emergency powers to handle the COVID-19 pandemic. Working groups continue to review and monitor guidance to ensure POL is compliant.	
9.4	**ATM Additional Business Rates Update:** a recent UK Supreme Court case has ruled that ATM facilities do not need to be assessed separately for business rates. POL has approximately 53 ATMS where claims can be made via an online system, however, only the occupier of the site can make the claim. In this instance, BOI would have to make the claim for POL backdated to 31 March 2018.	
9.5	**Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations**: public sector websites have a legal duty to make sure their websites meet accessibility requirements by 23 September 2020. Mobile apps are expected to be compliant by 23 June 2021. The digital innovation team believed POL's website was compliant and work was ongoing to meet the mobile applications compliance by the June 2021 deadline.	
9.6	The paper was **NOTED for onward submission to the ARC.**	
10.	**Policies for Approval:**	
	The following policies were **NOTED for onward submission to the ARC:** • Modern Slavery Statement: AK provided a more robust training regime had been implemented and that there was a greater understanding in the network about slavery/exploitation. JT highlighted the positive impact the branch support guide had provided to branches to highlight any issues of modern slavery and where to report these. • Anti-Bribery and Corruption Policy • Whistleblowing Policy • Financial Crime Policy • Anti -Money Laundering and Counter Terrorist Financing Policy • Document Retention Policy • Procurement Policy.	
11.	**Review of draft Audit, Risk and Compliance Committee meeting agenda for 27 July 2020**	
	The draft ARC agenda for 27 July was **NOTED**.	
12.	**Any other Business**	
	There was no other business.	