POL00423695

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	16 March 2021
Time:	10.00 - 13.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chair)	Johann Appel (Head of Internal Audit)
Helen Rhodes (Head of HR Organisation Effectiveness Project Lead) (deputising for 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)	Tom Lee (Financial Controller)
Cathy Mayor (Finance Director, Commercial)	Rebecca Whibley (Senior Assistant Company Secretary)
Jeff Smyth (Group Chief Information Officer)	Tony Jowett (Chief Information Security Officer): Item 5
	Peter Mitchell (Treasurer - Tax, Treasury and Supply Chain Finance): Item 6
	Sarah Gray (Group Legal Director): Item 7 & 8
	Jonny Lonsdale (Business Continuity Manager): Item 9
	Martin Hopcroft (Head of Health & Safety): Item 9
	Andrew Goddard (Managing Director, Payzone): Item 10
	Mark Siviter (Product Portfolio Director – Mails, Retail, PUDO & Gov services): Item 11
	Andy Kingham (Franchise Partnering Director): Item 11
	Dan Zinner (Group Chief Operations Officer): Item 12
	Emma Conroy (Interim Head of Strategic Partnerships): Item 12
	Tim Perkins (Service and Support Optimisation Director): Item 13
	Sally Smith (Money Laundering Reporting Officer & Head of Financial Crime): Item 14
	Barbara Brannon (Procurement Director): Item 15
Apologies:	

Dial In Details:

Join Microsoft Teams Meeting
GRO United Kingdom, London (Toll)
Conference ID: 264 657 434#
Pin (if applicable): 58042

Time		**Item**		**Owner**	**Action**
	1.	Welcome & Conflicts of Interest		Chairman	Noting
10.00	2.	Previous Meetings		Chairman	
		2.1	Minutes (12 January 2021)		Approval
		2.2	Action List		Discussion
10.05	3.	Combined Risk, Compliance and Audit Update			
10.05		3.1	Risk Report (dashboard)	Mark Baldock	Noting (onward submission to ARC)

Strictly Confidential

POL00423695

POST OFFICE LIMITED

10.15		3.2	Risk Appetite Statement: Legal & Compliance	Ben Foat & Jonathan Hill	Approval (onward submission to ARC)
10.25		3.3	Compliance Report	Jonathan Hill	Noting (onward submission to ARC)
10.35		3.4	Internal Audit Report	Johann Appel	Noting (onward submission to ARC)
10.45	4.	Internal Audit Plan 2021/22		Johann Appel	Noting & Approval (onward submission to ARC)
10.55	5.	IT Updates		Jeff Smyth/ Tony Jowett	Noting (onward submission to ARC)
10.55		5.1	PCI-DSS	Jeff Smyth	
11.05		5.2	Cyber Security	Tony Jowett	
11.15	6.	Foreign Currency and Hedging		Tom Lee & Peter Mitchell	Noting
11.25	7.	Bi-Annual Legal Risk Review (Non GLO/Starling)		Ben Foat/ Sarah Gray	Noting (onward submission to ARC)
11.35	8.	Law & Trends Update		Sarah Gray & Ben Foat	Noting (onward submission to ARC)
11.45	9.	Business Continuity		Jonny Lonsdale/Martin Hopcroft	Noting (onward submission to ARC)
11.55	10.	DeepDive: Payzone Governance		Andrew Goddard	Noting (onward submission to ARC)
12.05	11.	DeepDive: Dangerous Goods		Andy Kingham / Amanda Jones / Mark Siviter	Noting (onward submission to ARC)
12.15	12.	Strategic Partner Financial Stability Update		Emma Conway/Dan Zinner	Noting (onward submission to ARC)
12.25	13.	Procurement Compliance & Governance		Barbara Brannon	Noting (onward submission to ARC)
12.35	14.	Policies for Approval:		Jonathan Hill	Approval (onward submission to ARC)
		14.1	Summary Paper		
		14.2	Health & Safety		
		14.3	Procurement Policy		
12.40	15.	Postmaster Policies		Tim Perkins	Approval (onward submission to ARC)
		15.1	Guide to Policy Standards for Postmasters		
		15.2	Postmaster Complaints Handling Policy		

Strictly Confidential

POL00423695

POST OFFICE LIMITED

		15.3	Network Transaction Corrections Policy		
		15.4	Network Cash and Stock Management Policy		
		15.5	Postmaster Appeals Policy		
		15.6	Postmaster Training Policy		
		15.7	Postmaster Onboarding Policy		
12.50	16.	Whistleblowing Policy		Sally Smith	Discussion & Approval
12.55	17.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 30 March 2021		Chairman	Noting
13.00	18.	Any other business		Chairman	Noting
Next RCC Meeting: Tuesday 4 May 2021 at 10.00 to 13.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ					

Strictly Confidential

POL00423695

2.1

POST OFFICE LIMITED

MINUTES OF A MEETING OF THE RISK AND COMPLIANCE COMMITTEE OF POST OFFICE LIMITED HELD ON THURSDAY 12 JANUARY 2021 AT 10:00 VIA MICROSOFT TEAMS

Present:	**Attendees:**
Alisdair Cameron (Chairman) **(AC)**	Rob Wilkins (Cloud Services Director) **(RWI)**: Item 3.4 & 4
Lisa Cherry (Group Chief People Officer) **(LC)**	Tony Jowett (Chief Information Security Officer) **(TJ)**: Items 4 & 5
Ben Foat (Group General Counsel) **(BF)**	Russell Hancock (Supply Chain Director) **(RH)**: Item 6
Amanda Jones (Group Retail and Franchise Network Director) **(AJ)**	Sally Smith (Money Laundering Reporting Officer & Head of Financial Crime) **(SS)**: Item 7
Cathy Mayor (Finance Director, Commercial) **(CM)**	Maxine Cross (Head of Reward and Pensions): **(MC)**: Item 8
Jeff Smyth (Group Chief Information Officer) **(JS)**	Helen Rhodes (Head of HR Organisation Effectiveness, Project Lead) **(HR)**: Item 8
Regular Attendees:	Andy Jamieson (Head of Tax) **(AJ)**: Item 9
Johann Appel (Head of Internal Audit) **(JA)**	Tim Perkins (Service and Support Optimisation Director) **(TP)**: Items 10, 11 & 12
Mark Baldock (Head of Risk) **(MB)**	Declan Salter (GLO Director) **(DS)**: Item 13
Jonathan Hill (Compliance Director) **(JH)**	Graham Hemingway (Historical Matters Portfolio Lead) **(GH)**: Item 13
Tom Lee (Financial Controller) **(TL)**	Barbara Brannon (Procurement Director) **(BB)**: Item 16
Rebecca Whibley (Senior Assistant Company Secretary) **(RW)**	Sarah Gray (Group Legal Director) **(SG)**: Item 17
Apologies:	
N/A	

1.	**Welcome and Conflicts of Interest**	**Action**
	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 Committee meeting held on 12 November 2020 were **APPROVED**.	
2.2	Progress on completion of actions as shown on the action log was **NOTED** as follows: Action 1 from 12 November 2020 para 3.1 Risk, Compliance & Internal Audit Update - Risk Dashboard: These changes have not been made for January 2021 due to the Risk Team having moved off the RSA Archer system and are now building ServiceNow (IRM Pro) system. As such it was difficult to run Dashboards. The reporting in the new ServiceNow system would be built to take account of this action where possible. The action remained open. Action 2 from 12 November 2020 para 3.1 Risk, Compliance & Internal Audit Update - Risk Policy: These changes were made and the policy was approved by the Audit, Risk & Compliance Committee (ARC) at its meeting in November 2020 and then the Board in January 2021. The action was closed. Action 3 from 12 November 2020 para 3.3 Risk, Compliance & Internal Audit Update – Compliance Update (Anti-Bribery & Corruption Training): Current HR figure stands	

POL00423695

	at 92.4%, which includes contractors. Work was being undertaken to ensure contractors complete the training. The action was closed. Action 4 from 12 November 2020 para 3.3 Risk, Compliance & Internal Audit Update – Compliance Update (Access to Cash): The submitted version was sent by Martin Kearsley to the GE on Thursday 26th November 2020. The action was closed. Action 5 from 12 November 2020 para 3.4 Risk, Compliance & Internal Audit Update – Internal Audit (Effectiveness of the Second Line): A update on this work was contained within the Compliance Paper (see paragraph 3.3 below). A further update will be provided when further work has been undertaken. The action remained open. Action 6 from 12 November 2020 para 3.4 Risk, Compliance & Internal Audit Update – Internal Audit (Joiners, Movers, Leavers): IT have worked through the leavers and work was continuing on the movers. This work would be completed prior to the January 2021 ARC meeting. The action remained open. The Committee also requested that a list of what is required to be put together and for this to be tracked against for the next Committee meeting. Action 7 from 12 November 2020 para 3.4 Risk, Compliance & Internal Audit Update – Internal Audit (Actions): These changes were made to the report which was submitted to the ARC for its meeting in November 2020. A separate paper on the data privacy action was provided to the ARC for noting and it was agreed by the ARC that the management action would be revised in line with the solution that was presented to the ARC. The action due date will be re-set to 31 March 2021. The action was closed. Action 8 from 12 November 2020 para 3.4 Risk, Compliance & Internal Audit Update – Internal Audit (Special Investigation): A verbal briefing was provided in confidence to Al Cameron on 19 November. The action was closed. Action 9 from 12 November 2020 para 3.4 Risk, Compliance & Internal Audit Update – Internal Audit (Deletion of Data): Ben and Jeff have met to discuss the rules regarding data preservation in "legal-hold" situations and we have confirmed that there is no automatic deletion of any Outlook Email, SharePoint or OneDrive based data. Data access was deactivated in employee leaver situations but that data was still retrieval on request by line management or other authorised requestors. Data Protection have recommended that to keep within Post Office risk appetite that IT, in conjunction with Compliance, need to start working towards an initial purge of the emails systems and the implementation of an auto delete solution when the Legal Hold is removed. The action remained open. The Committee also requested that a clear plan of action was developed for the next Committee meeting. Action 10 from 12 November 2020 para 4.2 Cyber Security (Phishing Training): This will be provided to all GE members ahead of ARC paper submission on 18 January 2021. The action remained open. Committee commented that this list should be provided asap and that there should not be a reluctance to call people out when they have not completed mandatory training. Action 11 from 12 November 2020 para 4.2 Cyber Security (Phishing Comms): This was highlighted to the Leadership Group and mentioned in a 10@10. The action was closed. Action 12 from 12 November 2020 para 4.2 Cyber Security (ARC Paper Update): This was included in the paper for the ARC in November 2020. This action was closed.	**TJ** **BF/JH**

POL00423695

Action 13 from 12 November 2020 para 4.2 Cyber Security (Culture Shift): Initial meeting has been held with Juliet Lang in People team and plans are in development. An update will be provided at the March Committee meeting. The action remained open.

Action 14 from 12 November 2020 para 4.3 Joiners, Movers, Leavers: This was included in the paper for the ARC in November 2020. The action was closed.

Action 15 from 12 November 2020 para 4.4 Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing: This item is targeted to be presented to the GE for a decision on 20 January 2021. The action remained open.

Action 16 from 12 November 2020 para 5 Suspense Accounts: The ARC was asked to approve disclosure and felt it necessary to refer to the Board. This was therefore discussed and approved by the Board in November 2020. The action was closed.

Action 17 from 12 November 2020 para 6 Notification of Transaction Error: Since the last RCC, Post Office has completed a Request to Quote (RTQ) process and raised a Purchase Order for work to be completed to prevent duplicate auto transaction corrections from being issued in the future. This work would also include a non-related enhancement that will prevent any transaction correction narrative from being cut off after 500 characters. These enhancements would cost £9,860 and were due for completion by 19 March 2021. The action remained open.

Action 18 from 12 November 2020 para 8 Agreed Upon Procedures: This change was made to the paper which was submitted to the November 2020 ARC. The action was closed.

Action 19 from 12 November 2020 para 9 Historical Matters Unit (HMU) Governance Review: This change was made to the paper which was submitted to the November 2020 ARC. The action was closed.

Action 20 from 12 November 2020 para 11 Terms of Reference: These were approved at the December GE meeting and were available on the intranet and in the Diligent Reading Room. The action was closed.

Action 21 from 12 November 2020 para 12 Deepdive: Multiple partner financial stability update: Commercial Partners were faced with the same challenges of all retailers in this current climate, however, there were no significant concerns. Reduction in trading hours were being discussed with some Commercial Partners but none fall below the minimum/core trading hours. From the 1st January, WHSmith have reduced to core trading hours in 102 of their Post Offices (Monday to Friday 9am to 5:30pm; Saturday 9am to 12:30pm; Sunday closed) to ensure commercial viability, and a PO service offering. Increased hours would be reviewed in line with customer demand. In regard to resignations, CJ Lang (SPAR retailer) resigned on 28 of their Post Office branches during July/August last year, all but 4 of these would be closed this financial year. This was not driven by COVID-19, but the non-commercial viability of the PO in these sites. The retail continues to trade, and the PO would be replaced by a Food to Go offering. WHSmith have resigned on 10 of their Post Office branches, which has been driven by commercial terms not reaching agreement between WHSmith and their Landlord. Where commercial terms were agreed, WHSmith will renege on the Post Office termination. If no terms agreed, both the WHS retail and Post Office would close. Out of the 10 pending terminations five will close in Q4 (this financial year); three in Q1; one in Q3 and one in Q4 2022. With

POL00423695

	regard to the specific recourse for the closing branches, it has been confirmed that there is recourse for Post Office and this being worked through with Legal. The action was closed. Action 22 from 12 November 2020 para 16 Data Governance (Data Storage Contracts): Procurement have advised that the only providers are Box-It/Oasis & Postal Museum. The action was closed. Action 23 from 12 November 2020 para 16 Data Governance (Data Search): The action was set out in the Data paper that was noted by the ARC in November 2020 and was being actioned. An update was provided in the Compliance paper (see paragraph 3.3). The action was closed. Action 24 from 12 November 2020 para 16 Data Governance (Data Retention Policy Implementation): This was addressed in the Compliance paper (see paragraph 3.3). Progress was being made and the primary focus was to provide information as required for Group Litigation Order (GLO) disclosures on 5 February 2021 (deadline date for disclosure for the 41 past convictions referred for appeal by the CCRC to the Court of Appeal (Criminal Division)). A further update would be provided at the March Committee meeting. The action remained open. Action 25 from 12 November 2020 para 17 Procurement Governance & Compliance Report: This paper was prepared for the ARC and was shared offline with Lisa Harrington (only member of the Board who does not attend ARC meetings). The action was closed. Action 26 from 10 September 2020 para 4 Pensions Assurance: The Trustee has now received reconstructed pensionable pay and allowances data. This was being reviewed to assess both the differences to the 2017 data that formed the basis of the Rothesay buy-in and the quantum of the overpayments. A report was expected to be presented to the Trustee Board in March 2021 along with the Trustee rectification plans. The regulator has been updated and is expecting more information from POL at the end of the March. The action remained open. Action 27 from 13 July 2020 para 3.5 Compliance Report (Fairness): The Committee requested that this action remained open until such time that the sale of the business had been completed. The action therefore remained open. Action 28 from 13 July 2020 para 10.6 Money Laundering Reporting Officer (MLRO) Report: The HMRC supervisor who took over when the previous supervisor retired in May 2020 moved to a new role in the summer. A further supervisor was appointed in August 2020 and an initial virtual meeting has been held, but due to continuing COVID-19 restrictions, HMRC were not undertaking any supervisory visits or meetings, and it was unclear when this will recommence in 2021 or what the frequency or format of meetings will be with this new supervisor. The Committee requested that this action remained open, noting that there was also a requirement in the action to talk to retail on enforcing the three lines of defence and this needed to be done. The action therefore remained open. Action 29 from 11 November 2019 3.2 Supplier Contracts out of Governance (SSK): Commercial and legal negotiations were ongoing but were on track to complete a compliant support renewal of the legacy SSK estate by end of January. The action remained open.	

POL00423695

	Action 30 from 11 November 2019 3.2 Supplier Contracts out of Governance (Brands/RAPP): A compliant tender process has been run and the contract has been awarded to the incumbent provider, with operational costs reduced. The contract has been signed and is available on Web3. The action was closed.	
3.	**Risk, Compliance and Audit Update**	
	Risk	
3.1	Mark Baldock introduced the paper, which had been circulated previously and was taken as read. The following points were highlighted: - The report was an interim report as the team were presently moving from Archer to ServiceNow. The March Report would therefore have data from ServiceNow which was due to go live on 18 January 2021 and would be rolled out to the business in March/April (subject to the business case approval). - The paper gives helicopter review of big risk groups, alongside narrative round each risk - The paper also sought approval for the differentiation of risk reporting to the Board and the ARC. The proposal was that the Board would oversee enterprise risks with ARC focussing on policy compliance, trends and three lines of defence. This was discussed and it was agreed that the approach should more be about the nature of the risk concerned. ARC should deal with any risks relating to audit, controls or compliance. The Board should oversee risks relating to the commercial side of the business, including where regulatory changes might affect this. In the first instance this should be addressed at GE and then the Board if necessary. - It was requested that the report be updated to reflect the change in risk profile due to the signing of Master Distribution Agreement 2 (MDA2) with Royal Mail before it was submitted to the ARC. - Work was being undertaken to review the risks given the new purpose and the business was being challenged to explain the impact of each risk on Postmasters. It was also requested that a risk should be added about whether the business was doing enough on day-to-day support for Postmasters to ensure a network was sustained (for the March 2021 meeting). - Cathy Mayor questioned how the business could be encouraged to think about risks more regularly and proactively. Mark Baldock explained that this was phase two of his work and there would be a carrot and stick approach. The approach was to be presented to the Committee and the ARC in March 2021. The Chair noted that the Group Executive (GE) should also discuss this once a quarter. - Jeff Smyth also noted that there needed to be a specific risk around the Telco sale and behavioural changes this had caused for BAU. It was agreed Jeff and Mark Baldock would discuss this further for update a the March 2021 meeting. Accordingly, the Committee: i. **NOTED** the current status of key risks and Governance, Risk & Compliance (GRC) tool implementation; and ii. **APPROVED** an approach to the role of the Board and the RCC/ARC with respect to oversight of risk management that was issue based whereby: - the ARC would oversee risks relating to audit, controls or compliance; and - the Board would deal commercial risks; for onward submission to the ARC.	**MB** **MB** **MB** **MB/JS**
	Risk Appetite Statement: Legal & Compliance	
3.2	Ben Foat introduced the paper, which had been circulated previously and was taken as read, noting it was about the Risk Appetite for legal and regulatory risks, not risks for the Legal, Compliance and Governance directorate. The following points were discussed:	

POL00423695

	- Appendix A to the paper (setting out ARC approved Risk Appetite Scale) was conservative view of risk appetite and as such, the ARC would be asked to confirm it is content with this approach at its meeting on 26 January 2021. - The paper was still a work in progress to be finalised before submission to the ARC and it would also be submitted to the Chair prior to the ARC, as per her request. - The process to prepare the paper had been intensive and the Chair questioned how useful the document was for making decisions, given the effort involved. It was explained that it would not give an answer to each and every decision but it would provide a benchmark for decision-making. Jeff Smyth noted that the outcome needed to be real and actionable, modulated against how much recourse and investment was available to manage the risks identified. Ben Foat also highlighted that it must remain up-to-date and as such should be reviewed regularly to remain useful. - Lisa Cherry raised the People risks mentioned in the paper, specifically relating to Modern Slavery and payment of the minimum wage. The appetite was adverse to Modern Slavery (for example), but there was concern that this implied controls would be put in place which would require investment. However, the approach was more monitoring and as such there seemed to be a misalignment between the appetite and the action to be taken. Ben Foat explained that the position was that Post Office was adverse and, as there were criminal sanctions for Modern Slavery, controls needed to be put in place. The risk appetite discussion was useful in that it helped to draw out these issues. The Modern Slavery Statement was normally addressed in the autumn (which was too late to address the controls requirement) and as such, this should be addressed in the Risk Appetite Paper. Accordingly, the Committee **APPROVED** the draft corporate Legal & Compliance Risk Appetite Statements (subject to the points raised in its discussions) for onward submission to the ARC.	**BF**
	Compliance	
3.3	Jonathan Hill introduced the paper, which had been circulated previously and was taken as read. The following points were discussed: <u>Controls Framework</u>: The Chair and Ben Foat raised concerned about the lack of progress in this area and that there did not appear to be a coherent, funded programme. It needed to be on the prioritised Change list for next financial year and it was agreed the Chair, Ben Foat and Jonathan Hill would discuss further how the Framework would work for update at the next Committee meeting. The Chair stated that the Framework needed to be based on self-assessment by the Control owners. Jonathan Hill confirmed that this is the principle of the Framework, with assurance being provided by Compliance. Jonathan Hill explained: - That he has agreed with Tim Perkins and the new HMU Operations Director to accelerate the controls work with operations for completion in early February, pending the HMU's deep dive on process maps. - HMU was looking at what activities have been done to address individual points raised in the Common Issues Judgment (CIJ) and Horizon Issues Judgment (HIJ) and the Stamps work. - Process maps were also being built by the HMU team, but this took considerable time. building process maps. - Compliance was responsible for checking with business owners what controls were in place and ensuring that there was the right reporting/management	**AC/BF/JH**

POL00423695

	information (MI). The Controls Framework includes a guidance document to support business owners. The Chair requested that this work be fed into the Deloitte programme and requested that Jonathan Hill link in with the Chair, Ben Foat, Tom Lee and Johann Appel (for update at the next Committee meeting), asking the controls project should useServiceNow. Jeff Smyth also noted that IT were engaging with Procurement on sourcing support to enhance the IT controls infrastructure. It was agreed that there would be a collective decision on any support partner and Jonathan Hill was asked to discuss this with Jeff Smyth for update at the next Committee meeting. Data Management: The Chair highlighted the request to approve the recommendation to establish a Post Office-wide Data Governance framework and SteerCo, based on the Digital Data Governance framework but extended to encompass all forms of data. It was agreed that this was a matter for the GE and that a paper should be presented that sets out the purpose and how this could work (including the wider implications of the Framework, the cost and the accountabilities). Cookies: The Chair highlighted the request to approve the recommendation to assess the impact on Post Office's approach to cookies of new European regulatory rulings against Google and Amazon. Jonathan Hill explained that the suggestion was that the Digital and Compliance teams work together to consider the commercial implications of the rulings. It was agreed that this should be done, but that it was a commercial decision for Owen Woodley (Group Chief Commercial Officer) and, if necessary, the GE. Financial Services: Jonathan Hill was requested to provide the final report relating to Multi Principal Review of 1st line controls to the Committee before the next Committee meeting. Jonathan Hill was also asked to add deadlines to the agreed way forward for continuing with mystery shopping before the next Committee meeting. Accordingly the Committee **NOTED** the Compliance update, in particular: • The Controls Framework update; • The Data Management activities; • Post Office's approach to cookies; and; **APPROVED** the recommendation for the Digital and Compliance teams to assess the impact on Post Office's approach to cookies of new European regulatory rulings against Google and Amazon and that any decision on a change in approach was for Owen Woodley (Group Chief Commercial Officer) and, if necessary, the GE.	**JH** **JH** **JH** **JH**
	Internal Audit	
3.4	Johann Appel introduced the paper, which had been circulated previously and was taken as read. The following points were discussed: IT Control Framework: The five P2 audit actions were driven by absence of single individual and this has been mitigated by taking away the key person dependency. Mails and Parcels: The Chair raised a concern that it did not seem that someone was taking responsibility for these actions. Johann Appel explained that the actions were being discussed with Mark Siviter (Product Portfolio Director - Mails, PUDO, Retail	

POL00423695

	and Branch Identity Services) to try and make more specific. Johann Appel was asked to address this before the ARC or amend his paper to note that this report was not supported by the Committee. Historic Matters – CIJ Operations Improvement Programme (Interim Report): Johann Appel explained that the actions arising from this report were due to be completed by the end of February and if they were to go beyond this date, there needed to be a good reason and a clear timetable for completion. It was also noted that there were actually only two P1 actions outstanding and Johann Appel was asked to update the report with the latest action numbers and management comments before the January ARC meeting. In response to a questions from Ben Foat, Johann Appel confirmed that audit was also tracking the completion of the HMU actions, including the RACI model and it was highlighted that this needed to be within the next couple of weeks and not wait until March (when it was currently due). Belfast Exit Follow-up & PCI Compliance (Programme Assurance): Jeff Smyth explained that the management comment was in train. Post Office Insurance: The Chair felt that the summary table provided was not helpful and more detail as required as to the outcome of reports. It was agreed that the audit report rating would be added to the table and if the rating was adverse, there would be an explanation as to why. Audit actions: The majority of the actions were to be completed before the January 2021 ARC. The action to "agree the list of Crown Jewels with Post Office's GE" was to be done by Jeff Smyth before the January 2021 ARC meeting. Otherwise, the Committee **NOTED** the Internal Audit update, specifically progress being made with delivery of the Internal Audit programme and completion of audit actions.	**JA** **JA** **JA** **JS**
4.	**PCI-DSS and Cyber Security Update**	
	PCI-DSS Programme Update	
4.1	Rob Wilkins introduced the paper, which had been circulated previously and was taken as read. The following points were raised: - In response to a question from the Chair, it was confirmed that progress was being tracked by this Committee as it was a quasi-regulatory issue. - There was a major risk of Santander not responding in time for the May delivery date. This was an issue because Santander transactions could not be split out from those of other banks easily. It was requested that this be escalated by Cathy Mayor to Owen Woodley (Group Chief Commercial Officer) and Nick Read (Group CEO). It was also noted that this was to be discussed the GE on 13 January 2021. - The retail pilot was running successfully and the banking accreditation with Vocalink was also working well. Otherwise, the Committee **NOTED** the progress made since the last reporting period and the key risks as outlined in the paper.	**CM**
	Cyber Security	
4.2	Tony Jowett introduced the paper, which had been circulated previously and was taken as read. In response to questions from the Committee, Tony Jowett explained that Post Office was not particularly exposed to attacks similar to that of Solar Winds but more work was needed, including on the frequency of scanning the network and more data from Third Parties who attest they have scanned their networks. The	

POL00423695

	Crown Jewels analysis was also part of this work. Jeff Smyth noted that IT certainly wanted to do more and any projects would be added to the Change list for next year. Otherwise, the Committee **NOTED** the status and plans regarding the reduction of risk associated with Cyber Security including the Crown Jewels analysis for onward submission to ARC.	
	Joiners Movers Leavers (JML)	
4.3	Tony Jowett introduced the paper, which had been circulated previously and was taken as read. The Committee **NOTED** the status and plans regarding the reduction of risk associated with JML) – in particular those associated with Joiners during the current hybrid operating model for onward submission to the ARC, subject to the paper being updated to remind the ARC of the inherent risk across each JML area, how it has been reduced and what was still to do.	**TJ**
5.	**IT Controls Assessment**	
	Tony Jowett introduced the paper, which had been circulated previously and was taken as read. In response to a question from the Chair, it was explained that 10% of controls were not working, but ¾ these were not working because of the absence of a key person and not having a disaster recover manager in place. This had now been resolved. The Committee otherwise **NOTED** the status and plans regarding the reduction of risk associated with IT Controls for onward submission to the ARC.	
6.	**Supply Chain Historical IT Risks**	
	Russell Hancock introduced the paper, which had been circulated previously and was taken as read. The Chair questioned how the business can ensure there are no further instances of "off network" IT equipment being used and the following points were raised: - Tony Jowett explained that IT had started a scan of all Supply Chain locations as well as in person audits to check all equipment. - Jeff Smyth noted that there was a "bring out your dead" exercise and it was agreed that that a questionnaire would also be developed to ask the relevant locations what equipment they had in place and identify anything that might be "off network." It was flagged that these questions should include examples and be as simple as possible. It was further explained that ultimately it came down to whether the equipment was supported by the Post Office IT team. The key was to encourage vigilance. - Russell Hancock also suggested that Post Office IT equipment should include asset numbers as this would be a clear sign if something had not been provided centrally. - It was also highlighted that some of the supply chain teams still had discretionary spend and there needed to be increased governance around this. Unfortunately, monitoring the discretionary spend could not have been used to discover the present issue because the records did not go back far enough, but moving forwards this could be monitored. It was also confirmed that Data Protection team were engaged on the present issue. The Committee **NOTED** the issues highlighted, the steps being taken to identify and reduce any potential risks, **AGREED** the next steps and requested that a further update be provided to the Committee at its next meeting in March 2021.	**JS** **RH**

7.	**Money Laundering Annual Report**	
	Sally Smith introduced the paper, which had been circulated previously and was taken as read. The following points were discussed: - Resources: There were some resourcing issues within the Financial Crime team caused by (1) structural changes in the business meaning things that were no longer being picked up elsewhere and had to be picked up by the team and (2) a massive increase in issues within the general Financial Crime landscape (in December 2019 there were 219 Suspicious Activity Reports (SARs), but in December 2020 this figure stood at 700). The Committee felt that too much of the financial crime work was being centralised and it needed to be properly distributed within the business. As such, Lisa Cherry and Sally Smith were asked to discuss if there were enough people across the business with the accountability for Financial Crime controls, noting that it was the Financial Crime's team to simply check if these controls were good enough and report accordingly. - Banks & Money Service Businesses (MSBs): The 2020 National Risk Assessment (NRA) released in December 2020 had stated to quite a lot of noise and momentum for the banks to do more to prevent financial crime. In response to questions from the Chair, Sally Smith confirmed that responsibility for checking customers are genuine did rest with the banks, but Post Office, as a regulated entity, needed to demonstrate that it had controls in place to deal with high risk businesses. Work was being done on improving the mechanism by which the banks confirm that customers were genuine. It was requested that Sally Smith write to the banks and make it clear that MSBs cannot be used through the Post Office network. It was agreed that a deep dive on the issue was required. Both actions were to be updated for the next Committee meeting. - Capita: It had transpired that the contract was not clear on the ability to exit a reseller arrangement under Capita and the legal advice was that, as Capita had been using MSBs for a number of years, there was deemed acceptance of the practice. As such, commercial negotiations were required for the practice to cease. This was being undertaken by Alison McMullen (Payzone) and would be escalated to the GE-1 Contract Owner as required. Ben Foat requested to see the legal advice on the Capita contract. - Amazon Vouchers: The potential for these to be sold in a way that was being used fraudulently needed to be urgently addressed and accountability taken within the Bill Payments/Payzone team. Part of the issue was that the relationship was managed by Payzone and they did not have access to Post Office systems. This needed to be resolved. Cathy Mayor and Sally Smith were asked to follow up with Andrew Goddard and provide an update at the next Committee meeting. Sally Smith was also asked to ensure that the report properly addressed the three questions asked in the report within the conclusion and ensure that the actual remediation steps were articulated as well as the materiality and scale of each issue. This should be done prior to the report being submitted to the ARC. Jeff Smyth also questioned what controls under the PCI-DSS programme could be used to the support the financial crime controls work. It was agreed that Sally Smith and Jeff would meet to discuss this further, to update the Committee at its next meeting.	**LC/SS** **SS** **CM/SS** **SS** **SS/JS**

POL00423695

	Otherwise, the Committee: i. **NOTED** the annual report and its conclusions as part of its role in monitoring the adequacy and effectiveness of the Group's anti-money-laundering systems and controls which ensures Post Office's meets its regulatory obligations under the Money Laundering Regulations; and ii. **APPROVED** the recommendations within paragraphs 9 – 25 of this report and paragraph F of the Annual Report of the Money Laundering Reporting Officer, prior to the Annual Report being issued to our regulator, HMRC; for onward submission to the ARC (subject to the amendments as set out by the Committee in their discussions).	
8.	**HR Update**	
	Pensions Assurance	
8.1	Lisa Cherry introduced the paper, which had been circulated previously and was taken as read. The Chair raised concerns about the potential liability and timescales of this issue, noting that it might need to be escalated to Nick Read (Group CEO). Lisa Cherry explained that ultimately, the issue was caused by a Post Office mistake and as such, it was vital a good relationship with the Trustee was maintained. There was a Trustee meeting on 23 March 2021, which Lisa Cherry was attending and it is after this point that any escalation to Nick Read would be considered. The Chair also highlighted that the longer this was left, the greater the liability became and there needed to be communication with those affected. Maxine Cross explained that there was already a comms plan in place to advise those affected that there might be a problem. In addition Lisa Cherry was working closely with the team to ensure conversations were taking place at the right level with the CEO of the Trustees in advance of the Trustee Board meeting in March. Disclosures regarding the issue might need to be included in the Annual Report and Accounts and as such, comms would need to be released before such disclosures. The liability was not likely to be understood until March/April and the ARC Chair indicated that this might need to considered by the Board in April. Ben Foat also requested more information on the data and how far it went back. This was to be provided to Ben directly outside of the Committee before its next meeting in March 2021. The Committee otherwise **NOTED**: - the progress on Project Assurance, the programme of work to resolve the closed defined benefit scheme errors; - the progress against actions from the previous ARC; and - the continued reporting/dialogue with The Pensions Regulator (TPR); for onward submission to the ARC.	**LC/MC**
	Success Factors	
8.2	Lisa Cherry introduced the paper, which had been circulated previously and was taken as read. It was explained that the Success Factors system configuration was likely to cost £250,000 and this was already on the change list. It was noted that this was a legitimate cost as it was for improving controls and reducing errors. The Committee **NOTED** the progress of the process improvement work ongoing in People Shared Service Centre (PSSC) (including Success Factors) for onward submission to the ARC.	
9.	**Tax Update & Tax Strategy**	
	Andy Jamieson introduced the paper , which had been circulated previously and was taken as read. The Committee **NOTED** the Tax Update and **APPROVED** the annual review of the Tax Strategy for onward submission to the ARC.	
10.	**Update on branch losses and balances on Postmaster accounts**	

POL00423695

	Tim Perkins introduced the paper, which had been circulated previously and was taken as read. The Chair noted that there had been much improvement in this area and also praised Russell Hancock's team for their work on cash in this area. The following was raised: - A proper piece of analytical work was required to identify the route cause of discrepancies. The capability to do this was to be built within Tim Perkin's team but HMU were supporting. - There were numerous approved change budgets relating to service improvements for Postmasters and it was agreed that these budgets should be added together and an activity prioritisation list prepared such that the budget could be properly prioritised. It was noted that the Deloitte programme would be the overarching programme in this area, with smaller programmes under this. - Jeff Smyth highlighted that changes to Horizon were also needed. Tim Perkins explained that Simon Oldnall (Horizon & GLO IT Director) was already engaged on this and highlighted the need to get data all in one place such that checks for discrepancies could be run. - Jeff Smyth also noted that the thinking seemed to be solidifying quickly but the solution cost was not. This needed to be addressed quickly. Tim Perkins concurred, noting that the goal was to move to a proactive and preventative model. Otherwise, the Committee **NOTED** the update on balances posted to Postmaster customer accounts for onward submission to the ARC.	**AJ/TP**
11.	**Postmaster Policies**	
	Tim Perkins introduced the paper, which had been circulated previously and was taken as read. It was confirmed that: - The policies had been agreed with HMU, the National Federation of Sub-Postmasters (NFSP) and Legal, Compliance and Governance (LCG). - The policies were broad with the underlying processes being narrower. - Approval of these policies would close off some outstanding actions within the Internal Audit Common Issues Judgement report. It was agreed that the operationalisation of the policies was key and Tim Perkins would provide an update on the controls implemented to the Committee at its next meeting. The following policies were **APPROVED** for onward submission to the ARC: • Postmaster Account Support Policy; • Postmaster Accounting Dispute Resolution Policy; and • Network Monitoring and Audit Support Policy; and that, moving forwards, these policies be reviewed and approved annually by the Committee only.	**TP**
12.	**Mails Fraud Update**	
	Tim Perkins introduced the paper, which had been circulated previously and was taken as read. Two points were discussed: - There was a sense that Post Office was always "coming from behind" when identifying these issues and there needed to be analytical capability in house to support identification. Tim Perkins explained that change funding had been assigned and consideration was being given as to how to procure the best people for this work. Johann Appel also explained that his team were currently recruitment a data analytical manager who could support this work. Tim Perkins, Jeff Smyth and the Chair agreed to discuss the need for more	**TP/JS/AC**

POL00423695

	analytical capability with Dan Zinner (Group Chief Operations Officer) and provide an update to the Committee at its next meeting. - Post Office was now dependent on Royal Mail to continue the investigation (to allow Horizon data to be consolidated against the actual mail) and as yet they had not provided a date as to when this investigation would be conducted. Accordingly, the Committee **NOTED** a mails fraud identified on 25 November 2020 through a whistleblow received by an Area Manager from a member of staff in an agency Post Office.	
13.	**Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority**	
	Graham Hemingway introduced the paper, which had been circulated previously and was taken as read. It was highlighted that: - The action relating to responsibilities, accountabilities and decision-making authorities (including the extent of delegation of authority) to be clarified via completion of a RACI matrix was ongoing due to discussions with UK Government Investments (UKGI) and the Department of Business, Energy and Industrial Strategy (BEIS). It was thought this would be ready for the ARC on 26 January 2021 and it was requested that the matrix was sent to the Committee before being submitted to the ARC. - In response to questions from the Committee, it was explained that risks by workstream were reported to the Board and Declan Salter was to report to the GE once a month. As such it was agreed that this topic need not be reported through to this Committee and the ARC, but that the GE report should include risk and controls. Otherwise, the Committee **NOTED** how are risks relating to fraudulent claims being managed in the Historical Shortfall Scheme (and the Stamps Scheme) and that controls are in place to confirm the eligibility of claims for onward submission to the ARC.	**GH** **DS/GH**
14.	**Policies for Approval**	
	Jonathan Hill presented the paper, which had been circulated previously and was taken as read. The following was highlighted: - Cyber and Information Security Policy: This was a regular annual update with minor changes included in the updated policy. - Vetting Policy: The original has been considerably updated and split out into two separate policies for employees and Postmasters/Assistants as the vetting procedures were considerably different. - Investigations Policy: This was a significant revision. The policy set the minimum standards for investigation practices across the business and where there were other specific policies which specific requirements (i.e. relating to Postmasters) those policies would take precedence. An investigations group would be set up to create effective minimum control standards and management information (MI). The following policies were **APPROVED** for onward submission to the ARC: - Cyber & Information Security; - Investigations (subject to Jonathan Hill/Ben Foat checking the reference to reporting concerns to the CEO as raised by Amanda Jones); and - Employee, Postmaster & Postmaster Assistant Vetting Requirements (subject to the policy being reviewed to ensure that the job titles included were up-to-date following the recent restructure).	**JH/BF** **JH**
15.	**Subsidiary Policy Mandate**	

POL00423695

	Jonathan Hill presented the paper, which had been circulated previously and was taken as read. It was explained that all Group Policies were, by default, to be adopted by Post Office's subsidiaries unless there was a legal, regulatory or other material reason why they could not. It was also confirmed that Payzone were presently working through the Group Policies to establish which could be adopted. The Payzone Board had discussed the adoption of policies and concluded that Payzone should not adopt different policies to those of the Group where at all possible. Lisa Cherry also highlighted that it must be clear that Post Office Limited only People policies should not apply to subsidiaries, although this would be addressed by being clear that the mandate applied to Group Policies only. It was agreed that this would be rectified before the paper was presented to the ARC. Otherwise, the Committee **APPROVED** the following Subsidiary Policy Mandate: i. Subsidiaries must adopt all Group Policies unless it cannot do so for a legal, regulatory or other material reason; ii. Where subsidiaries cannot adopt a Group Policy for one of the above reasons, subsidiary shall adopt its own policy in that area that is aligned to the Group Policy; iii. This adapted subsidiary policy must be reviewed and approved by the Post Office Limited (POL) Compliance team and the POL Policy Owner, who shall confirm alignment to the Group Policy; and iv. This process would not apply to Post Office Insurance (POI) regulatory policies, being Risk, Conduct Risk, Vulnerable Customers, Ex Gratia, Remuneration and any other policies as required by the Financial Conduct Authority (FCA). Where these policies are adopted by the POI Board, the Company Secretariat shall notify POL Compliance of the adoption such that their records can be updated; for onward submission to the ARC (subject to the amendment of the paper to define "Group Policy" within the paper).	**JH**
16.	**Procurement Compliance & Governance**	
	Barbara Brannon presented the paper, which had been circulated previously and was taken as read. It was highlighted that the GE were due to discuss the proposed nine month extension to the contract for Cheque Processing for Postal Orders and Camelot, which was required to make the contract co-terminus with the existing Corporate Banking contract as the would be operational issues if the services from separated. The Corporate Banking contract was due to be re-procured in Q3 2021 and the cheque processing services would be brought within the scope of this re-procurement. Overall, Procurement Compliance was an improving area. The Committee **NOTED** the Procurement Compliance & Governance report specifically, the Procurement Risk Exceptions submitted to the Post Office Limited Group Executive and Board since November 2020 and the contracts in the Procurement pipeline.	
17.	**Law & Trends Update**	
	Ben Foat presented the paper, which had been circulated previously and was taken as read. The following was highlighted: - New guidance has been published on Data Subject Access Requests - (DSARs) and there was "stop the clock" provision which allowed the business to ask questions of requestees - The London Interbank Offered Rate ("LIBOR") would change to Sterling Overnight Indexed Average ("SONIA") later in 2021, which would have an impact on commercial loan agreements. - There were some areas of concern which were being monitored relating to property litigation.	

POL00423695

	The Committee **NOTED** the Law & Trends report and the new or proposed material changes to laws and regulations since its last meeting for onward submission to the ARC.	
18.	**Review of draft Audit, Risk and Compliance Committee meeting agenda for 26 January 2021**	
	The draft ARC agenda for 26 January 2021 was **NOTED**. The Chair suggested that the Mails Fraud paper could be noted at the ARC (without presentation) if the ARC Chair agreed.	
19.	**Any other Business**	
	There was no other business.	

DRAFT

POL00423695

Post Office Limited
Risk & Compliance Committee
OPEN ACTIONS

No.	Meeting Date	Minute Reference	Action	Action Owner	Due Date	Comment
1	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	March 2021 ARC (update at May 2021 RCC) ~~Update @ March 2021 RCC (resolution by end of January 2021)~~ ~~Update @ January 2021 RCC (resolution by end of January 2021)~~	09/03/2021: Commercial negotiations did not conclude as planned due to GDPR complexities and the contract has been extended on an interim basis again to end March. The completed contract was received on Monday is now awaiting review and approval from POL legal. This review is expected to complete prior to 22nd March in order that the risk is closed by the submittal of the ARC paper. Further update to be provided at the next Committee meeting. 22/01/2021: Cathy Mayor removed from Action Owner as no longer within her area. 05/01/2021: Commercial and legal negotiations are ongoing but are on track to complete a compliant support renewal of the legacy SSK estate by January end. 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.
2	14/01/2020	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 @ May 2021 RCC Meeting ~~Update @ March 2021 RCC Meeting~~ ~~Update @ January 2021 RCC Meeting~~	09/03/2021: HMRC are still not conducting any meetings. 12/01/2021: The Committee requested that the action remained open. 31/12/2020: The HMRC supervisor who took over when the previous supervisor retired in May 2020 moved to a new role in the summer. A further supervisor was appointed in August 2020 and an initial virtual meeting has been held, but due to continuing Covid restrictions, HMRC are not undertaking any supervisory visits or meetings, and it is unclear when this will recommence in 2021 or what the frequency or format of meetings will be with this new supervisor. 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.
3	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	09/03/2021: The Telco sale is due to complete on 15/03/2021 and this will be confirmed at the meeting. Provided this is confirmed, this action is **recommended for closure.** 12/01/2021: The Committee requested this action remained open until the sale was complete. 23/12/2020: This action is no longer required given the sale of the telco business due in January 2021. 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.*"

POL00423695

4	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 @ May 2021 RCC Meeting ~~Update @ March 2021 RCC Meeting~~ ~~Update @ January 2021 RCC Meeting~~ ~~September~~	09/03/2021: We have sent RMPP what we believe to be final data. This will form the basis for the Trustee's report to the Trustee Board on 23rd March. We have requested advanced sight of the data to be presented. This is expected to give us initial view of the quantum of the errors. We are preparing a paper for Project Assurance Steerco on 8th April that will bring together the data our obligations and wider considerations so that an approach to discussions with the Trustee can be agreed. A further update will be provided at the next Committee meeting. 05/01/2021: The Trustee has now received reconstructed pensionable pay and allowances data. This is being reviewed to assess both the differences to the 2017 data that formed the basis of the Rothesay buy-in and the quantum of the overpayments. A report is expected to be presented to the Trustee Board in March 2021 along with the Trustee rectification plans. The regulator has been updated and is expecting more information from POL at the end of the March. 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. [redacted]	COMPLETE
5	12/11/2020	3.1 Risk Compliance & Audit Update	**Risk Dashboard**: The Chair highlighted that the dashboard needed to better highlight any changes in risk vs. the ongoing management of an existing risk. Ben Foat further commented that risk scores were given but the numbers were not defined. It was also highlighted that Declan Salter should be identified against the GLO risk and the impact score for the Starling and GLO risk should be five, not three. It was agreed that Mark Baldock would make these changes to the risk dashboard, including putting any new risks to the front of the dashboard moving forwards (from January 2021) and provide a verbal update on these elements to the Audit, Risk & Compliance Committee (ARC) in November.	Mark Baldock	March RCC & ARC 2021 ~~January RCC & ARC 2021~~	10/03/2021: Updated Dashboard tabled for RCC/ARC in 3/2021 with data derived directly from ServiceNow following successful data migration of Post Office risk data set in 1/2021. Draft format shared with ARC Chair. Format will be flexed in light of changing needs and requirements. **Recommended for closure.** 06/01/2021: These changes have not been made for January 2021 due to the Risk Team having moved off the RSA Archer system and are now building ServiceNow (IRM Pro) system. As such it is difficult to run Dashboards. The reporting in the new ServiceNow system will be built to take account of this action where possible. 30/11/2020: A verbal update was provided to the ARC as required.	
6	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Effectiveness of the Second Line during COVID-19: Ben Foat questioned whether the work being undertaken to put a Controls Framework in place was happening quick enough, noting there had been some delays in getting the project to the Project Review Board. The audit report emphasised that there could not be any more delays. It was agreed that this work should be taken to GE to discuss the need to develop the Framework and the approach that should be taken.	Johan Appel/Ben Foat/Jonathan Hill/CoSec (agenda)	Further update to be provided at May 2021 RCC ~~Further update to be provided at March 2021 RCC~~ ~~ASAP with update to be provided @ January 2021 RCC~~	08/03/2021: An update on this work is contained within the Compliance paper to be presented on 16th March 2021. Please also refer to Action 19). However this work has been paused and is not expected to restart for c.six months. Accordingly, the action is **recommended for closure**, with further updates in the Compliance Paper in due course. 05/01/2021: A update on this work is contained within the Compliance Paper to be presented to the Committee on 12 January 2021. A further update will be provided when further work has been undertaken. 30/11/2020: Rebecca Whibley has flagged to CoSec team for GE agenda. Johann Appel/Jonathan Hill to advise of timing and provide paper. A whole project has been set up to push this forward and actions are already underway on GLO-related matters. A formal project plan is being built in parallel to the activities being done as we have just been getting on with it. Also, a business case is being created for submission in January to cover the whole of Post Office. An update will be provided in January 2021.	
7	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Joiners, Movers & Leavers (JML): The Chair stressed the importance of completing this work. The risks for internal movers needed to be mapped and resolved. Lisa Cherry was asked to take this away.	Helen Rhodes & Tony Jowett ~~Lisa Cherry~~	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	09/03/2021: The IT actions for this have now been completed with no discrepancies reported. HR have also confirmed this is complete. **Recommended for closure.** 05/01/2021: IT have worked through the leavers and work is continuing on the movers. This work will be completed prior to the January 2021 ARC meeting. 03/12/2020:This work is being carried out by Tony Jowett and Helen Rhodes.	

POL00423695

8	12/11/2020	3.4 Risk, Compliance & Audit Update	**Internal Audit:** Further, it was requested that: Ben Foat and Jeff Smyth discuss offline the rules around deleting/not deleting data for legal reasons.	Ben Foat & Jeff Smyth	Update to be provided @ May 2021 RCC ~~Update to be provided @ March 2021 RCC~~ ~~Update to be provided @ January 2021 RCC~~	08/03/21: Further action by IT to create an auto-delete capability is subject to funding, which will be reviewed during 2021/22. 06/01/2021: Ben and Jeff have met to discuss the rules regarding data preservation in "legal-hold" situations and we have confirmed that there is no automatic deletion of any Outlook Email, Sharepoint or Onedrive based data. Data access is deactivated in employee leaver situations but that data is still retrieval on request by line management or other authorised requestors. Data Protection have recommended that to keep within POL risk appetite that IT, in conjunction with Compliance, need to start working towards an initial purge of the emails systems and the implementation of an auto delete solution when the Legal Hold is removed.
9	12/11/2020	4.2 Cyber Security	**Cyber Security:** It was requested that Tony Jowett provide a list of all individuals who have not done the phishing training to the relevant GE members.	Tony Jowett	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	02/02/2021: This list was provided as requested. **Recommended for closure.** 05/01/2021: This will be provided to all GE members ahead of ARC paper submission on 18 January 2021.
10	12/11/2020	4.2 Cyber Security	**Cyber Security:** Tony Jowett also noted that his team were looking at tool to monitor culture shift and it was agreed that he would liaise with HR on the on-going culture work to build this into the business' longer term defence plans.	Tony Jowett	Update to be provided @ March 2021 RCC ~~ASAP with update to be provided @ January 2021 RCC~~	10/03/2021: The next steps on culture/cyber awareness are now factored into the planning for the 21/22 Cyber programme described in March paper. Recommended for closure. 05/01/2021: Initial meeting has been held with Juliet Lang in People team and plans are in development. An update will be provided at the March Committee meeting.
11	12/11/2020	4.4 Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing	**Belfast Data Center (Horizon) Disaster Recovery Post Test Briefing**: The current plan was to not to do another test of this size and scale this financial year but to ensure that as part of Belfast Exit there was equivalent activity in suitable point i.e. latter point of the next calendar year. The Chair commented that this was one of the business' biggest risks and felt that another test should be done at Easter given the recent test was only partially successful. Jeff Smyth explained that the test was expensive (circa £75,000) and also destroys all change programme activity hosted in the secondary data center. The Chair noted that £75k was a tiny sum compared to the cost and reputational damage of losing branch trading. It was agreed that the GE should agree the timing of the next test.	Gary Walker / CoSec (agenda)	Update to be provided @ March 2021 RCC ~~Update to be provided @ January 2021 RCC~~	10/03/2021: The proposal was put into Jeff and Jeff agreed to schedule the next DR at a time in June which coincides with a opportune time in the Belfast exit programme and a least invasive time in the PCI-DSS programme. (June) There is some further discussion around the dates now given some of the milestones in these projects will be moved but rest assured that the DR testing will remain in the same place (relative to milestones) for those two programmes. In addition, we are also now looking at doing further testing between now and the full DR test to ensure that more assessment of resiliency is done (as far as practically possible) in parallel to the programmes in question. **Recommended for closure.** 06/01/2021: This item is targeted to be presented to the GE for a decision before the end of January 2021. 30/11/2020: Rebecca Whibley has flagged to CoSec team for GE agenda. Gary Walker to advise of timing and provide paper.
12	12/11/2020	6. Notification of Transaction Error	**Notification of Transaction Error:** It was agreed that the outcome of the investigation into the error should be published in the interests of transparency (Tim Perkins to arrange).	Tim Perkins	Update to be provided @ May 2021 RCC ~~Update to be provided @ January 2021 RCC~~	10/03/2021: The changes required in CFS have been agreed with Finance and Accenture. The date for completion is to be confirmed (should be confirmed by RCC), but will be later than 19/03/2021 as indicated in previous updates. The subsequent Branch Focus article will also be delayed. Further update to be provided at the May RCC. 12/01/2021: The Committee requested this action remained open. 17/12/2020: 1.Since the last RCC, Post Office has completed an RTQ process and raised a Purchase Order for work to be completed to prevent duplicate auto transaction corrections from being issued in the future. This work will also include a non-related enhancement that will prevent any transaction correction narrative from being cut off after 500 characters. These enhancements will cost £9,860 and are due for completion by 19/03/2021. 2.Once these enhancements are completed, a Branch Focus article will be published to explain the enhancements and to give Postmasters reassurance that when Post Office identifies issues that impact them, it will respond by clearly publicising the issue and making changes that ensure the issue cannot recur. Given the expected completion date for the enhancements, the Branch Focus article should be published in late March 2021.

POL00423695

13	12/11/2020	16. Data Governance	**Data Governance:** Accordingly, the Legal, Data Protection, IT and Ruk Shah (MI & Analytics Director) were asked to work on a coherent recommendation on how the data retention policy should evolve and how it will be implemented. This should return to the RCC and ARC in January 2021. Further, the current paper needed to articulate the next steps and process that will be worked through.	Ben Foat, Jeff Smyth, Jonathan Hill (delegated to Chris Russell)	Update @ May 2021 RCC ~~Update @ March 2021 RCC January 2021 RCC & ARC (paper update for November 2020 ARC)~~	05/03/2021: This will be addressed in Compliance Paper to be presented to the Committee in March 06/01/2021: This is addressed in the Compliance paper to be presented to the Committee on 12 January 2021. Progress is being made and the primary focus is to provide information as required for GLO disclosures on 5 February 2021 (deadline date for disclosure for the 41 past convictions referred for appeal by the CCRC to the Court of Appeal (Criminal Division)). A further update will be provided at the March Committee meeting. 30/11/2020: The Data Governance paper was updated as requested and submitted to the November 2020 ARC for noting.
14	12/01/2021	3.1 Risk Update	**Risk Update:** It was requested that the report be updated to reflect the change in risk profile due to the signing of Master Distribution Agreement 2 (MDA2) with Royal Mail before it was submitted to the ARC	Mark Baldock	January 2021 ARC	10/03/2021: Risk rating was reduced to 4:2 in line with signing of MDA2. **Recommended for closure.**
15	12/01/2021	3.1 Risk Update	**Risk Update:** Work was being undertaken to review the risks given the new purpose and the business was being challenged to explain the impact of each risk on Postmasters. It was also requested that a risk should be added about whether the business was doing enough on day-to-day support for Postmasters to ensure a network was sustained (for the March 2021 meeting).	Mark Baldock	May 2021 RCC/ARC ~~March 2021 RCC/ARC~~	10/03/2021: This was is ongoing: Central Risk are currently supporting Retail & Franchise Network in the identification of intermediate and local postmaster-centric risks (as well as existing risks that that have impact postmasters). Update dataset to be included on GRC in next reporting period. The aim is for this to be underpinned but appetite statement on which ARC approval will be sought in 5/2021
16	12/01/2021	3.1 Risk Update	**Risk Update:** Cathy Mayor questioned how the business could be encouraged to think about risks more regularly and proactively. Mark Baldock explained that this was phase two of his work and there would be a carrot and stick approach. The approach was to be presented to the Committee and the ARC in March 2021. The Chair noted that the Group Executive (GE) should also discuss this once a quarter.	Mark Baldock	March 2021 RCC/ARC	10/03/2021: Business Case approval being sought for GRC Phase 2 rollout from 4/2021. This will support the rollout of risk management capacity to all Business Unit Heads and Risk Owners thereby ensuring accountability is positioned appropriately. There will be a requirement for Risk Owners to their review their risks every 2 months to allow for accurate RCC/ARC updates . **Recommended for closure.**
17	12/01/2021	3.1 Risk Update	**Risk Update:** Jeff Smyth also noted that there needed to be a specific risk around the Telco sale and behavioural changes this had caused for BAU. It was agreed Jeff and Mark Baldock would discuss this further for update a the March 2021 meeting.	Mark Baldock	March 2021 RCC/ARC	10/03/2021: Propose to close: In light of Telco sale the status of all associated risks have been changed to 'inactive.' **Recommended for closure.**
18	12/01/2021	3.2 Legal & Compliance Risk Appetite	**Legal & Compliance Risk Appetite Paper**: Lisa Cherry raised the People risks mentioned in the paper, specifically relating to Modern Slavery and payment of the minimum wage. The appetite was adverse to Modern Slavery (for example), but there was concern that this implied controls would be put in place which would require investment. However, the approach was more monitoring and as such there seemed to be a misalignment between the appetite and the action to be taken [redacted]	Ben Foat	March 2021 RCC/ARC ~~January 2021 ARC~~	09/03/2021: Legal & Compliance risk appetite update paper tabled for RCC/ARC 3/2021 meetings which provides advice on how the approach to risk appetite would address the challenges around Modern Slavery risks. **Recommended for closure.**
19	12/01/2021	3.3 Compliance Update	**Controls Framework:** The Chair and Ben Foat raised concerned about the lack of progress in this area and that there did not appear to be a coherent, funded programme. It needed to be on the prioritised Change list for next financial year and it was agreed the Chair, Ben Foat and Jonathan Hill would discuss further how the Framework would work for update at the next Committee meeting. The Chair stated that the Framework needed to be based on self-assessment by the Control owners. Jonathan Hill confirmed that this is the principle of the Framework, with assurance being provided by Compliance.	Ben Foat/Jonathan Hill/Al Cameron	Update @ May 2021 RCC/ARC ~~Update @ March 2021 RCC/ARC~~	06/03/2021: An update on this work is contained within the Compliance paper to be presented on 16th January 2021 [please also refer to Action 6]. However this work has been paused and is not expected to restart for c.six months. Accordingly, the action is **recommended for closure**, with further updates in the Compliance Paper in due course.
20	12/01/2021	3.3 Compliance Update	**Data Management:** The Chair highlighted the request to approve the recommendation to establish a Post Office-wide Data Governance framework and SteerCo, based on the Digital Data Governance framework but extended to encompass all forms of data. It was agreed that this was a matter for the GE and that a paper should be presented that sets out the purpose and how this could work (including the wider implications of the Framework, the cost and the accountabilities).	Jonathan Hill (Matthew Warren)	Update @ May 2021 RCC/ARC ~~Update @ March 2021 RCC/ARC~~	09/03/2021: The Data Governance steerco is already established for the data strand and is up and running. We are currently in the process of recruiting a dedicated Data Governance lead role. This person will take over the ownership of data governance and pick up the initial work already conducted in this area e.g identification of data owners / stewards / SME's etc. Further update to be provided at the next Committee meeting.

2.2

POL00423695

21	12/01/2021	3.3 Compliance Update	**Cookies**: The Chair highlighted the request to approve the recommendation to assess the impact on Post Office's approach to cookies of new European regulatory rulings against Google and Amazon. Jonathan Hill explained that the suggestion was that the Digital and Compliance teams work together to consider the commercial implications of the rulings. It was agreed that this should be done, but that it was a commercial decision for Owen Woodley (Group Chief Commercial Officer) and, if necessary, the GE.	Jonathan Hill	Update @ March 2021 RCC/ARC	09/03/2021: An update is provided in the Compliance report. **Recommended for closure.**
22	12/01/2021	3.3 Compliance Update	**Financial Services:** Jonathan Hill was requested to provide the final report relating to Multi Principal Review of 1st line controls to the Committee before the next Committee meeting.	Jonathan Hill	May 2021 RCC/ARC ~~March 2021 RCC/ARC~~	09/03/2021: We are still awaiting the first draft of this review from our Principals, we have chased for a response, which is expected within the next 2 weeks. Further update to be provided at the next Committee meeting.
23	12/01/2021	3.3 Compliance Update	**Financial Services:** Jonathan Hill was also asked to add deadlines to the agreed way forward for continuing with mystery shopping before the next Committee meeting.	Jonathan Hill	March 2021 RCC/ARC	09/03/2021: An update is provided in the Compliance report. **Recommended for closure.**
24	12/01/2021	3.4 Internal Audit	**Mails and Parcels:** The Chair raised a concern that it did not seem that someone was taking responsibility for these actions. Johann Appel explained that the actions were being discussed with Mark Siviter (Product Portfolio Director – Mails, PUDO, Retail and Branch Identity Services) to try and make more specific. Johann Appel was asked to address this before the ARC or amend his paper to note that this report was not supported by the Committee.	Johann Appel	January 2021 ARC	22/01/2021: More detailed actions were agreed with Mark Siviter and the report was re-circulated. **Recommended for closure.**
25	12/01/2021	3.4 Internal Audit	**Historic Matters – CTI Operations Improvement Programme (Interim Report):** Johann Appel explained that the actions arising from this report were due to be completed by the end of February and if they were to go beyond this date, there needed to be a good reason and a clear timetable for completion. It was also noted that there were actually only two P1 actions outstanding and Johann Appel was asked to update the report with the latest action numbers and management comments before the January ARC meeting.	Johann Appel	January 2021 ARC	22/01/2021: Management comment was added for the ARC summary and the report was updated to reflect the latest status. A verbal update will be provided at the ARC to reflect any further progress. IA now track and report the remaining actions on a weekly basis. **Recommended for closure.**
26	12/01/2021	3.4 Internal Audit	**Post Office Insurance:** The Chair felt that the summary table provided was not helpful and more detail as required as to the outcome of reports. It was agreed that the audit report rating would be added to the table and if the rating was adverse, there would be an explanation as to why.	Johann Appel	January 2021 ARC	22/01/2021: Audit report rating has been included in the table. **Recommended for closure.**
27	12/01/2021	3.4 Internal Audit	**Audit actions:** The majority of the actions were to be completed before the January 2021 ARC. The action to "agree the list of Crown Jewels with Post Office's GE" was to be done by Jeff Smyth before the January 2021 ARC meeting.	Jeff Smyth	Before January 2021 ARC	10/03/2021: GE have provided their approval of baseline crown jewel systems. No further follow-up action required as update process is triggered by retirement/implementation of key systems to baseline inventory. **Recommended for closure.**
28	12/01/2021	4.1 PCI-DSS Update	**PCI-DSS Update:** There was a major risk of Santander not responding in time for the May delivery date. This was an issue because Santander transactions could not be split out from those of other banks easily. It was requested that this be escalated by Cathy Mayor to Owen Woodley (Group Chief Commercial Officer) and Nick Read (Group CEO). It was also noted that this was to be discussed the GE on 13 January 2021.	Cathy Mayor (Owen Woodley)	Update @ March 2021 RCC	10/03/2021: This risk has been closed off by the tech team in discussion with Santander tech team. They confirm that Santander service will continue even while migration for the dedicated link to the common Vocalink connection is undertaken, and all banks (including Santander) can continue to use existing transaction types – so no change required from any bank. **Recommended for closure.**
29	12/01/2021	4.3 Joiners, Movers, Leavers	**Joiners, Movers, Leavers**: The Committee NOTED the status and plans regarding the reduction of risk associated with JML) – in particular those associated with Joiners during the current hybrid operating model for onward submission to the ARC, subject to the paper being updated to remind the ARC of the inherent risk across each JML area, how it has been reduced and what was still to do.	Tony Jowett	January 2021 ARC	02/02/2021: The paper was updated as requested prior to submission to the ARC on 26 January 2021. **Recommended for closure.**
30	12/01/2021	6. Supply Chain Historical IT Risks	**Supply Chain Historical IT Risks:** Jeff Smyth noted that there was a "bring out your dead" exercise and it was agreed that that a questionnaire would also be developed to ask the relevant locations what equipment they had in place and identify anything that might be "off network." It was flagged that these questions should include examples and be as simple as possible. It was further explained that ultimately it came down to whether the equipment was supported by the Post Office IT team. The key was to encourage vigilance.	Jeff Smyth	Update @ May 2021 RCC ~~Update @ March 2021 RCC~~	10/03/2021: IT have developed a "shadow IT" questionnaire and are testing this approach locally within IT. This activity will be completed by 30th April 2021. We will then progressively use the same "amnesty and sweep" approach across the wider business to determine scale and importance of non-IT supported systems. Report back to May RCC on IT progress findings with a proposal for how to rollout across wider business.

POL00423695

31	12/01/2021	6. Supply Chain Historical IT Risks	**Supply Chain Historical IT Risks:** The Committee NOTED the issues highlighted, the steps being taken to identify and reduce any potential risks, AGREED the next steps and requested that a further update be provided to the Committee at its next meeting in March 2021.	Russell Hancock	March 2021 RCC	09/03/2021: Following on from the previous update given to RCC in January, KPMG who undertook forensic examination of the impacted PCs have found that no external access had been made to the devices. As a result no compromise of PO data has occurred and no breach of any GDPR obligations. KPMG made recommendations around password security and ensuring the business had a robust asset register of all IT assets in order to ensure that this issue could not be repeated again. The SC / IT review of all SC sites has not uncovered any further breaches and as such no further actions are required. **Recommended for closure.**
32	12/01/2021	7. Annual Money Laundering Report	**Resources:** There were some resourcing issues within the Financial Crime team caused by (1) structural changes in the business meaning things that were no longer being picked up elsewhere and had to be picked up by the team and (2) a massive increase in issues within the general Financial Crime landscape (in December 2019 there were 219 Suspicious Activity Reports (SARs), but in December 2020 this figure stood at 700). The Committee felt that too much of the financial crime work was being centralised and it needed to be properly distributed within the business. As such, Lisa Cherry and Sally Smith were asked to discuss if there were enough people across the business with the accountability for Financial Crime controls, noting that it was the Financial Crime's team to simply check if these controls were good enough and report accordingly.	Lisa Cherry / Sally Smith	Update @ March 2021 RCC	09/03/2021: Meeting held between Lisa Cherry, Jon Hill and Sally Smith to discuss pressures caused by recent structural changes and impacts to team, together with increasing workloads caused by changing criminal behaviours – there was alignment that there were resource requirements and that these did sit within Financial Crime. **Recommended for closure.**
33	12/01/2021	7. Annual Money Laundering Report	**Banks & Money Service Businesses (MSBs):** The 2020 National Risk Assessment (NRA) released in December 2020 had stated to quite a lot of noise and momentum for the banks to do more to prevent financial crime. In response to questions from the Chair, Sally Smith confirmed that responsibility for checking customers are genuine did rest with the banks, but Post Office, as a regulated entity, needed to demonstrate that it had controls in place to deal with high risk businesses. Work was being done on improving the mechanism by which the banks confirm that customers were genuine. It was requested that Sally Smith write to the banks and make it clear that MSBs cannot be used through the Post Office network. It was agreed that a deep dive on the issue was required. Both actions were to be updated for the next Committee meeting.	Sally Smith	Update @ May 2021 RCC ~~Update @ March 2021 RCC~~	09/03/2021: Following the last meeting, there has been more movement at an industry level on driving focus on resolving the issues with cash deposits, with several banks now being more proactive and have tightened their controls. Martin Kearsley and Sally Smith have had several meetings with UK Finance, and the NECC Project Admiralty is now meeting monthly. The NECC are also meeting with UK Finance and Sally Smith to discuss further ways to drive control improvements. At this stage, the issue with MSBs has not been raised specifically with the banks, as if they implement required controls, this ceases to be an issue for Post Office. We are also aware of ongoing Law Enforcement/Regulator activity with certain MSBs which will likely result in better controls. A further update will be provided to the next Committee meeting.
34	12/01/2021	7. Annual Money Laundering Report	**Amazon Vouchers:** The potential for these to be sold in a way that was being used fraudulently needed to be urgently addressed and accountability taken within the Bill Payments/Payzone team. Part of the issue was that the relationship was managed by Payzone and they did not have access to Post Office systems. This needed to be resolved. Cathy Mayor and Sally Smith were asked to follow up with Andrew Goddard and provide an update at the next Committee meeting.	Sally Smith/Cathy Mayor (Andrew Goddard)	Update @ May 2021 RCC ~~Update @ March 2021 RCC~~	09/03/2021: PZBP are progressing changes, but do not yet have implementation dates (Kevin Meredith is assisting PZBP with raising the system changes via Service Now, as PZBP do not have access), transactional changes and limits to the product are also being pursued by EPay, but they have not yet confirmed date of changes. Financial Crime have requested that PZBP press EPay for a delivery date, or 'pause' sales of the product. PZBPL Update: Weekly meetings are scheduled with the FC team are ongoing to ensure progression. Talks with epay and Amazon regarding fraud mitigations are continuing with feedback expected for the next meeting. A ticket has been raised with Service Now for a pop up message. A further update will be provided to the next Committee meeting.
35	12/01/2021	7. Annual Money Laundering Report	**MLRO Report:** Sally Smith was also asked to ensure that the report properly addressed the three questions asked in the report within the conclusion and ensure that the actual remediation steps were articulated as well as the materiality and scale of each issue. This should be done prior to the report being submitted to the ARC.	Sally Smith	January 2021 ARC	09/03/2021: This was addressed in ARC report in January. **Recommended for closure.**
36	12/01/2021	7. Annual Money Laundering Report	**PCI-DSS & Financial Crime:** Jeff Smyth also questioned what controls under the PCI-DSS programme could be used to the support the financial crime controls work. It was agreed that Sally Smith and Jeff would meet to discuss this further, to update the Committee at its next meeting.	Sally Smith/Jeff Smyth	Update @ March 2021 RCC	09/03/2021: Session held (JS/SS and team) to understand types of data analysis that the team perform. As part of data platform activity (sponsored by myself and Al), we will incorporate the Financial Crime Team "use cases" into the overall platform demand plan. Their needs will be prioritised versus other business demand. We anticipate requirements gathering/analysis phase will occur in FY21Q1, although this is subject to Investment Committee funding prioritisations. **Recommended for closure.**

POL00423695

37	12/01/2021	8. Pensions Assurance	**Pensions Assurance**: Ben Foat also requested more information on the data and how far it went back. This was to be provided to Ben directly outside of the Committee before its next meeting in March 2021.	Lisa Cherry/Maxine Cross	Before March 2021 RCC	09/03/2021: David Scothern replied to Ben on 22 January since then we have what we expect to be final data and can now add: The pensionable pay data shows errors that date back to 2014 and contains both overpayments and underpayments. Important: It should be noted that this is data on pensionable pay and allowances. This data will need to be processed by RMPP administrators to convert it into pension benefits. RMPP processes include the application of various underpins so errors in pensionable pay data do not necessarily become errors in pension benefits. **Recommended for closure.**
38	12/01/2021	10. Update on branch losses and balances on Postmaster accounts	**Change Spend:** There were numerous approved change budgets relating to service improvements for Postmasters and it was agreed that these budgets should be added together and an activity prioritisation list prepared such that the budget could be properly prioritised. It was noted that the Deloitte programme would be the overarching programme in this area, with smaller programmes under this.	Amanda Jones/Tim Perkins	Update @ March 2021 RCC	10/03/2021: The change budgets relating to service improvements, and including the Deloitte work, have all been put under a single programme of work (Postmaster Service Improvement Programme) and this programme has been approved at PRB and IC. The programme will manage prioritisation of activities taking its lead from the Deloitte work. **Recommended for closure.**
39	12/01/2021	12. Mails Fraud Update	**Analytical Capability:** There was a sense that Post Office was always "coming from behind" when identifying these issues and there needed to be analytical capability in house to support identification. Tim Perkins explained that change funding had been assigned and consideration was being given as to how to procure the best people for this work. Johann Appel also explained that his team were currently recruitment a data analytical manager who could support this work. Tim Perkins, Jeff Smyth and the Chair agreed to discuss the need for more analytical capability with Dan Zinner (Group Chief Operations Officer) and provide an update to the Committee at its next meeting.	Tim Perkins/Jeff Smyth/Al Cameron	Update @ May 2021 RCC ~~Update @ March 2021 RCC~~	10/03/2021: The scope for this work is being looked at in the wider context of a forensic capability being stood up within Horizon IT; There are natural synergies around the set of capabilities to provide analytical services across a broad range processes and these can leverage off the work being looked at around rapid surfacing if transactional data. Further update to be provided in May 2021.
40	12/01/2021	13. Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority	**RACI Matrix:** The action relating to responsibilities, accountabilities and decision-making authorities (including the extent of delegation of authority) to be clarified via completion of a RACI matrix was ongoing due to discussions with UK Government Investments (UKGI) and the Department of Business, Energy and Industrial Strategy (BEIS). It was thought this would be ready for the ARC on 26 January 2021 and it was requested that the matrix was sent to the Committee before being submitted to the ARC.	Graham Hemingway	Update @ May 2021 RCC ~~Prior to January 2021 ARC~~	09/03/2021: A draft RACID matrix was shared with Historical Matters Committee on 18 February 2021 and with GE w/c 22 February 2021. Additionally, draft RACID shared with internal audit for feedback. Feedback from CFO is being reviewed and discussions are ongoing with Finance and with Strategy and Transformation Director relating to governance arrangements which will then be incorporated into an updated RACID.
41	12/01/2021	13. Historical Matters Unit: Fraudulent Claims Controls & Delegation of Authority	**HMU GE Report:** In response to questions from the Committee, it was explained that risks by workstream were reported to the Board and Declan Salter was to report to the GE once a month. As such it was agreed that this topic need not be reported through to this Committee and the ARC, but that the GE report should include risk and controls	Graham Hemingway / Declan Salter	Next GE report, Update @ March 2021 RCC	09/03/2021: HM GE reports to contain risks and controls. Risk Log for Scheme additionally shared with UKGI and top risks reviewed at monthly monitoring meetings. Programme updates for each workstream are included in the reading room for every Board submission. DS calls-out any issues in his monthly report for both GE and Board. **Recommended for closure.**
42	12/01/2021	14. Policies for Approval	**Investigations Policy:** The following policies were APPROVED for onward submission to the ARC: -Investigations (subject to Jonathan Hill/Ben Foat checking the reference to reporting concerns to the CEO as raised by Amanda Jones); and	Jonathan Hill/Ben Foat	Prior to January 2021 ARC	22/01/2021: This was corrected prior to submission to the ARC. **Recommended for closure.**
43	12/01/2021	14. Policies for Approval	**Vetting Policies:** The following policies were APPROVED for onward submission to the ARC: - Employee, Postmaster & Postmaster Assistant Vetting Requirements (subject to the policy being reviewed to ensure that the job titles included were up-to-date following the recent restructure).	Jonathan Hill	Prior to January 2021 ARC	22/01/2021: This was corrected prior to submission to the ARC. **Recommended for closure.**
44	12/01/2021	15. Subsidiary Policy Mandate	**Subsidiary Policy Mandate**: Jonathan Hill presented the paper, which had been circulated previously and was taken as read. It was explained that all Group Policies were, by default, to be adopted by Post Office's subsidiaries unless there was a legal, regulatory or other material reason why they could not. It was also confirmed that Payzone were presently working through the Group Policies to establish which could be adopted. The Payzone Board had discussed the adoption of policies and concluded that Payzone should not adopt different policies to those of the Group where at all possible. Lisa Cherry also highlighted that it must be clear that Post Office Limited only People policies should not apply to subsidiaries, although this would be addressed by being clear that the mandate applied to Group Policies only. It was agreed that this would be rectified before the paper was presented to the ARC.	Jonathan Hill	Prior to January 2021 ARC	22/01/2021: This was corrected prior to submission to the ARC. **Recommended for closure.**

POL00423695

Central Risk Dashboard

RCC

16 March 2021

Strictly Confidential

POL00423695

1. Overview

Summary

Risk Status

556 active risks (14 enterprise, 90 intermediate, 453 Local). 6 risks rated 20 including:
Commercial (Customer requirements not met): Risk existing/emerging requirements of Post Office (new and existing) customers across the various sectors are not met such that customer demand declines rapidly
People (Industrial Action (DMB): Risk of DMB IA in 6-7/2021 and/or 'go-slow'. Dispute resolution in place including GOLD teams to mitigate. CWU conversations ongoing to ensure transparency.
External Fraud: Given substantial levels of cash and stock in Network risk of fraud being carried out by external parties.
H&S: Risk to postmasters & supply chain employees' mental and physical safety given their visibility and accessibility and the ongoing demands of the pandemic. Safety video on Branch Hub and increasing the number of Health Check calls to branches.

Other Risk activity

Strategy: risk dataset to be reviewed in light of launch of revised Strategy in 4/2021, – do not anticipate major changes
Future of the Workplace: Review of emerging risks as a result of plans for post-pandemic return to the workplace
Postmaster-centric risks: work underway to recalibrate some existing risks to articulate more clearly postmaster impact
HMU: Early set of HMU risks now included in risk data set. Work ongoing
People: HR proactively reviewing their risk data set. Updated data to be included in next reporting period
Telco: following sale majority of Telco risks now inactive
POI: looking to migrate POI risks data onto ServiceNow over next few weeks
CSR: Working with Comms to ensure all existing risks with CSR impact articulated accordingly – will provide business with a thematic view

Risk Appetite

LCG risk appetite update paper tabled for RCC/ARC 3/2021 meetings. Following initial noting, formal ARC approval now sought on approach. Initial supporting KRIs identified, along with potential data sources and indicative tolerances. Plan to including latest LCG appetite and KRI trends in standard RCC/ARC Dashboard from 5/2021.
In discussion with Retail and Franchise Network around Operational risk appetite (given this will cover postmaster-centric risks). Plan is get to an internally agreed position by end of 3/2021 with ARC approval sought in 5/2021.

ServiceNow GRC Phases 1 & 2

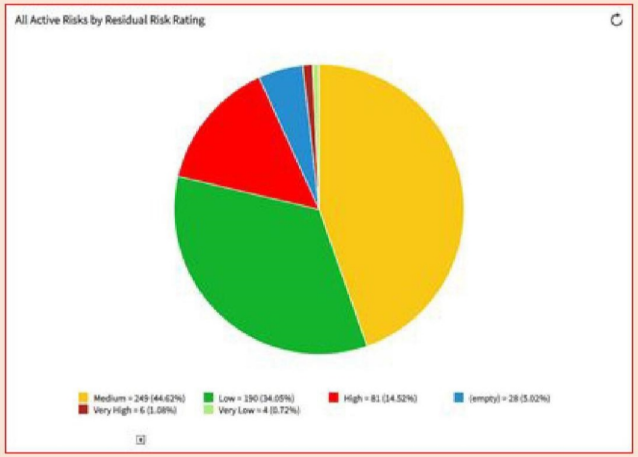
Phase 1 completed on time in 1/2021. 550+ risks migrated from RSA Archer to Service Now GRC platform. Central Risk initial training on product. Training material (Slides, Quick Reference Cards, Videos and supporting processes) nears sign-off. Will support wider deployment.

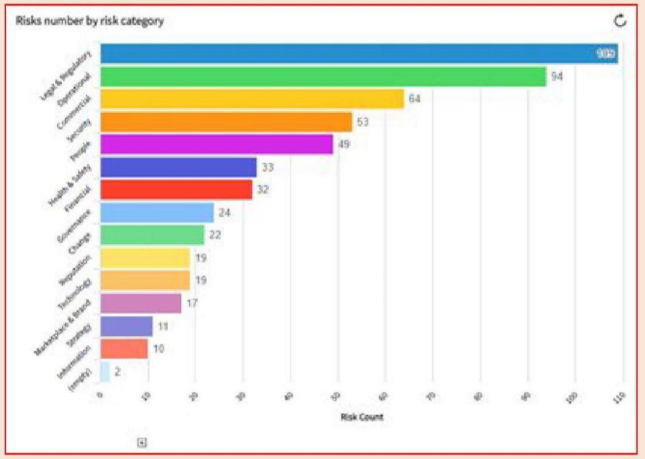
Phase 2 Business Case finalised (including enterprise licence). Subject to internal approval will allow rollout of risk capability across the business (over 4-5 months) and the onboarding of Finance, IT and SPO controls. Rollout targeting 4-10/2021 period. Initial pilot in 4/2021 (IT, Comms and Legal seen as potential candidates). Standard controls user requirement nears sign-off. Will allow GRC tool to support the onboarding of additional controls emanating from Compliance-led wider Control Review.

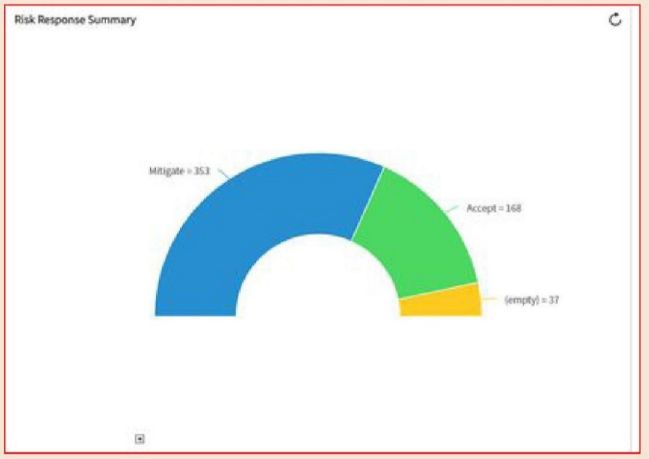
Strictly Confidential

POL00423695

2. Ratings, Categories & Response







Summary

Residual Ratings: Banding satisfactory. Will be assuring 6 very high risk ratings are compliant and, if so, secure detailed mitigations. 28 risks have no rating. These are in the Tech/Security space as just been added to the system. Now being addressed.

Risk Category: Shows 109 risks (of 556) are in Legal & Regulatory space. Although recent risk appetite work has seen an increase in the number of such risks classification to be reviewed in next report. It is expected this will result in a more equitable spread across the categories. Cross-thematic report to be included in next Dashboard.

Risk Response: 168 risks have an 'accept' response. Need to align this with the RAS. In most cases the residual rating is low but some are not. Challenging in next reporting period.

17 risks do not have a response – the majority are result of internal risk transfer where importing business unit need to formally reconfirm response. To be addressed in next period.

Strictly Confidential

POL00423695

3. Risk numbers

Summary

This table provides a corporate 'horizontal' view of the Post Office's 556 active risks **by number**. The 'x' axis lists the individual GE Commands with the 'Y' axis providing the enterprise risk categories.

Key headlines

- This is work in progress and is influenced by the accuracy of risk allocation (by GE Group and individual classification). Central Risk now assuring this data so there may be some further recalibration
- Group Commercial: has a material number of Legal & Regulatory risks (generally in the non-compliance space)
- Group Finance: a reasonable spread but interestingly has no Change or Technology risks
- General Counsel: not surprisingly has a significant number of Legal risks in part influenced by the recent work on appetite. Central Risk will be check this allocation
- Group Information: a high proportion of risks are in the (cyber) security space
- Group Operations: a material number of change related risks but little classified as operations as these are picked up within Retail & Franchise Network
- Group People: a reasonably equitable spread
- Group Historical Matters: very light on the number of identified risks. Central Risk in proactive discussions to ensure increased articulation in the next reporting period.

Post Office Risks Number (by GE command and Enterprise Category)

Category \ Business Unit	Group Commercial	Group Finance	Group General Counsel	Group Information	Group Operations	Group People	Group Retail & Franchise Network	Group Corporate Affairs, Communications & Brand	Group Historic Matters	Post Office	Count
Change	1	0	0	0	18	1	1	0	0	1	22
Commercial	45	2	0	14	1	0	0	1	0	1	64
Financial	5	21	0	0	2	0	3	0	0	1	32
Governance	1	12	8	0	0	1	0	0	1	1	24
Health & Safety	0	19	0	0	0	7	6	0	0	1	33
Information	0	5	0	1	1	1	1	0	0	1	10
Legal & Regulatory	27	8	63	0	0	3	5	0	2	1	109
Marketplace & Brand	13	0	0	2	0	0	0	1	0	1	17
Operational	8	38	3	10	3	1	29	0	1	1	94
People	3	4	3	2	0	29	7	0	0	1	49
Reputation	2	1	0	0	0	0	1	13	1	1	19
Security	1	2	0	45	0	0	4	0	0	1	53
Strategy	2	3	0	0	3	2	0	0	0	1	11
Technology	0	0	0	15	0	3	0	0	0	1	19
Sum	108	115	77	89	28	48	57	15	5	14	556

Strictly Confidential

POL00423695

4. Risk weighting

Summary

This table complements the earlier table by providing a corporate 'horizontal' view of the Post Office's 556 active risks but this time by **average risk rating** (i.e. a summary total of the individual risk ratings divided by the number of risks). The 'x' axis lists the individual GE Commands with the 'Y' axis providing the enterprise risk categories.

Key headlines

- As before this is work in progress as the data is influenced by the accuracy of risk allocation. Central Risk now fully assuring this data so there may be some recalibration at end of the next period
- Group Commercial: their 108 risks are equitably spread but have a higher weight in the Financial, Security and Strategy space
- Group Retail & Franchise : their 57 risk have a higher risk weighting in H&S, Legal and People in part because of the work underway around postmaster risks
- Group Historical Matters: even though very light on the number of risks the risk weight is relatively high compared to other GE Groups. This is not surprising and is likely to increase as more risks get articulated.

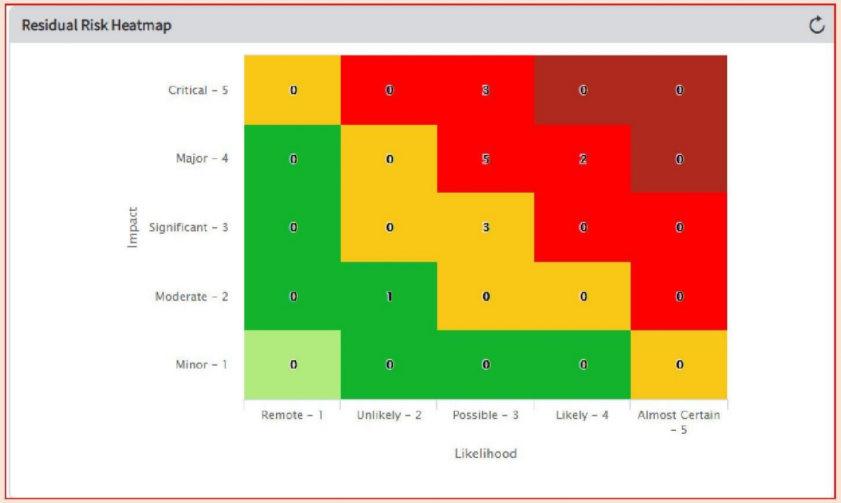
Post Office Risks Number (by GE command and Enterprise Category)

Category \ Business Unit	Group Commercial	Group Finance	Group General Counsel	Group Information	Group Operations	Group People	Group Retail & Franchise Network	Group Corporate Affairs, Communications & Brand	Group Historic Matters	Post Office	Group
(empty)							9				9
Change	6				8	9	9			9	8
Commercial	6	6	5	7	9					16	7
Financial	10	8	5		11		8			15	9
Governance	6	6	5			6			12	4	6
Health & Safety		9	5			7	16			16	9
Information		7	5		4	8				9	7
Legal & Regulatory	6	7	6	8		6	14		15	15	6
Mkt.place & Brand	9		6							12	6
Operational	6	6	6	10		12	7		8	12	7
People	7	5	5			6	10			12	6
Reputation	5	2					8	6	12	12	6
Security	10	10		8			6			9	8
Strategy	10	7	6		6	7				12	9
Technology			6	10		7				15	8
Average	6	6	6	8	5	6	10	6	13	12	7

Strictly Confidential

POL00423695

5. Enterprise Risks: Summary



Risk #	Risk Owner	Enterprise Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Jan-20]	Latest Residual RAG (I/L) [Mar-21]	Trend
RK0 020 005	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.	(4/4)	(4/4)	(4/4)	⇨
RK0 020 008	Martin Hopcroft	**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)	(4/4)	(4/4)	⇨
RK0 020 006	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)	⇨
RK0 020 010	Ben Foat	**Legal:** Risk the Post Office is unable to comply with legislative and regulatory changes.	(5/3)	(5/3)	(5/3)	⇨
RK0 020 017	Gary Walker	**Technology**: Risk that the Post Office is unable to deliver a new Front Office system and has an ineffective Disaster Recovery regime.	(5/3)	(5/3)	(5/3)	⇨
RK0 020 014	Richard Taylor	**Reputation**: Risk that the Post Office reputation becomes severely damaged as a result of perceived ethical violations and/or adverse stance to corporate social responsibility	(4/3)	(4/3)	(4/3)	⇨
RK0 020 011	Owen Woodley	**Marketplace and Brand**: Risk the demand for Post Office services and products across the various sectors declines and/or loyalty to the Brand reduces.	(5/4)	(4/3)	(4/3)	⇨

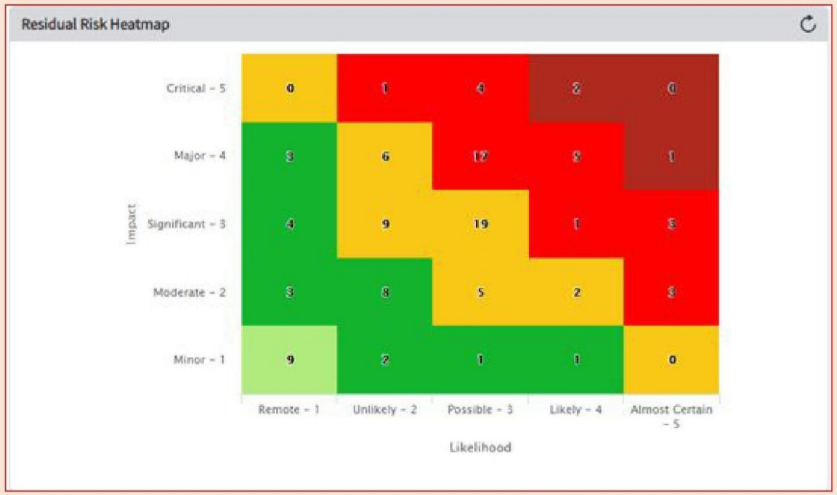
Summary

14 enterprise risks of which 11 have a rating of 16+. These risks are the apex of the overall risk data set with their ratings shaped directly by their downstream risks and the effectiveness of their mitigating activity. These risks tend to get managed through the aggregated activity at the intermediate and local level. Key risks in this area include:
Commercial: Risks the Commercial proposition is unattractive because existing products are too complex or confusing, new products are cost ineffective, unable to be scaled and unattractive to the market.
Health & Safety: Because of external H&S events (e.g. pandemic), detrimental business activities and/or external factors there is a risk that the Post Office business and its staff are adversely impacted.
Financial: Risks the Post Office has insufficient funding and/or uncontrolled costs in the short-, medium and long-term such it is unable to deliver its strategic objectives.
Legal: Risks the Post Office is unable to comply with legislative and regulatory obligations and/or the outcome of other external legal activity (i.e. litigation, Disputes).

Strictly Confidential

POL00423695

6. Intermediate Risks: Summary



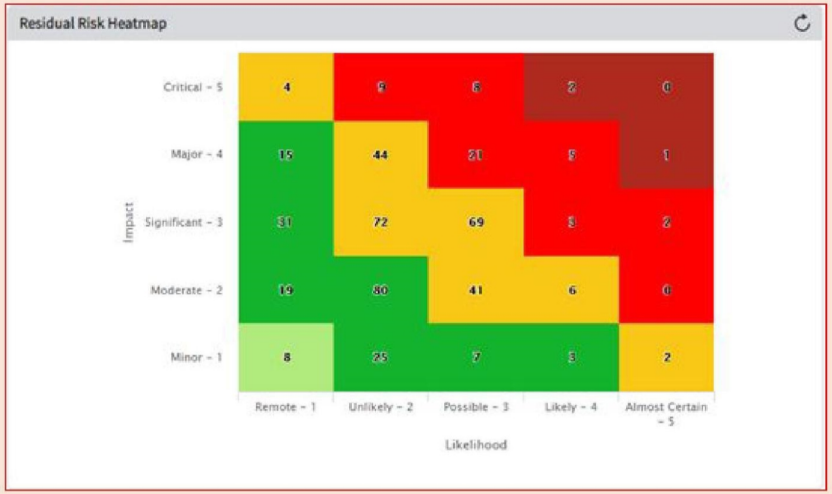
Risk #	Risk Owner	Business Unit	Enterprise Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Jan-20]	Latest Residual RAG (I/L) [Mar-21]	Trend
RK0 020 064	Henk Van Hulle	Group Commercial	**Customer requirements not met**: Risk the existing and emerging requirements of Post Office (new and existing) customers across the various sectors are not met.	(5/4)	(5/4)	(5/4)	⇨
RK0 020 074	Ed Dutton	Group Commercial	**Non-compliance with Pricing Super-Complaint FCA notice**: Risk that POI is not ready or has misjudged the outcome.	(5/4)	(3/3)	(5/4)	⇧
RK0 020 085	Mark Siviter	Group Commercial	**Failure of ID Services to meet customer need**: Risk that the Post Office may not be able to offer a relevant ID Service which meets customer need and remains relevant to the market.	(5/4)	(5/4)	(5/4)	⇨
RK0 020 034	Ed Dutton	Group Commercial	**POI product sales below forecast**: Risk that Post Office Insurance product sales remain significantly below forecast.	(4/4)	(4/4)	(4/4)	⇨
RK0 020 622	Ed Dutton	Group Commercial	**Decline in Network Engagement**: Risk that a decline in network engagement leads to a significant loss of low-cost acquisition leads from the branch channel.	(5/4)	(4/4)	(4/4)	⇨
RK0 020 079	Henk Van Hulle	Group Commercial	**Reduced income from Digital products and services:** Risk that Post Office digital products and services income is materially reduced when compared to physical products and services.	(5/4)	(4/4)	(4/4)	⇨
RK0 020 019	Ed Dutton	Group Commercial	**Insufficient POI EBITDAS**: Risk that Post Office Insurance EBITDAS contribution is significantly below forecast	(5/4)	(4/4)	(4/4)	⇨

Summary

90 intermediate risks of which 37 have a rating of 16+ including:
POI (Non-compliance with Pricing Super-Complaint): Risk that POI is not ready for new FCA price walking regime rules go live. Central Risk working with the business on detailed mitigation plan. POI Board paper on dealing with FCA changes and winning within market. Key controls include project plan, project quality control and development of strategy for maximising return within the market. .
POI: Risk Post Office Insurance product sales remain significantly below forecast resulting in reduced revenue Travel product back on sale. Significant uncertainty remains around rate of recovery. quarantine restrictions increase doubt. Branch sales continue to be at low level.
Commercial (Customer requirements not met): Risk existing/emerging requirements of Post Office (new and existing) customers across the various sectors are not met such that customer demand declines rapidly. Central Risk working with the business on detailed mitigation plan
Commercial (ID Services): Risk may not be able to offer a relevant ID Service if requisite Government funding is not forthcoming. Reviewing a faster roll out of the tablet services to ensure ready for the travel bounce-back period. Discussing an awareness campaign with Marketing. Regular meetings with Government Departments on role PO can play

POL00423695

7. Local Risks: Summary



Risk #	Risk Owner	Department	Enterprise Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Jan-20]	Latest Residual RAG (I/L) [Mar-21]	Trend
RK0020405	Tim Perkins	Service & Support Optimisation	**Mental and physical health and safety through crime such as, violence and hate crime**: Risk to their mental and physical safety through crime such as, violence and hate crime.	(5/4)	(5/4)	(5/4)	→
RK0020388	Tim Perkins	Service & Support Optimisation	**External fraud**: Risk of fraud being carried out by external parties.	(5/4)	(5/4)	(5/4)	→
RK0020188	Max Jacobi	Financial Performance & Business Analysis	**Insufficient liquidity (COVID & BREXIT)**: Risk that Post Office is facing months of exceptionally poor trading conditions.	(4/4)	(4/4)	(4/4)	→
RK0020162	Andrew Kingham	Franchise Partnering	**Health and Safety Breach - Branch Network**: Risk of harm or breach of regulatory requirements.	(5/4)	(5/4)	(4/4)	↓
RK0020579	Tim Perkins	Service & Support Optimisation	**Non-compliance with GLO findings**: Risk of non-compliance with the findings of the GLO across Postmaster.	(4/4)	(4/2)	(4/4)	↑
RK0020524	Brian Kelly	Tax & Treasury	**Net Liabilities**: Risk that the group may enter a position of Net Liabilities	(4/4)	(4/4)	(4/4)	→
RK0020066	Declan Salter	HM Legal	**Historical Matters overturned convictions**: Risk that the Post Office is perceived as dishonest, disrespectful or incompetent in its dealings with its employees, Agents, partners and/or customers	(5/4)	(5/3)	(5/3)	→

Summary

453 local risks of which 51 have a rating of 16+ including:
H&S: Risk to postmasters & supply chain employees' mental and physical safety given their visibility and accessibility and the demand of the pandemic . Safety video on Branch Hub and increasing the number of Health Check calls to branches.
Net Liabilities: Risk that Group may enter a position of Net Liabilities which may trigger a number of events such as default on commercial agreements and funding arrangements. Situation is being closely monitored along with pre-emptive action for impacted arrangements if required
Non-compliance with GLO (Service Support) findings: Rating recalibrated this period. Mitigations include removal of maintained error limits, removal of Limit on settling centrally <£150, review of ATM transaction corrections and investigation of Camelot data integrity issue.
Historical Matters overturned convictions: Because of ongoing Group Litigation actions the Post Office is perceived as dishonest, disrespectful or incompetent in its dealings with its employees, Agents, partners and/or customers which leads to loss of sales and and/or increased costs through fines and legal fees.

Strictly Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.2

Title:	Corporate Legal & Compliance Risk Appetites: An Update	**Meeting Date:**	16 March 2021
Author:	Jonathan Hill, Director of Compliance Sarah Gray, Group Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting & Approval

The Risk & Compliance Committee (RCC) is asked to:

i. note the latest position on the Post Office's appetite to corporate Legal & Compliance risks and our response to the comments provided by RCC/ARC in 1/2021, and along with our proposed Next Steps and timeline;

ii. approve the Post Office's appetite position to corporate Legal & Compliance risks,

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

Executive Summary

RCC/ARC are asked to **note** we

- [redacted]

RCC/ARC are asked, in light of the above, to **approve** the Post Office's appetite position to corporate Legal & Compliance risks.

Confidential & Legally Privileged

POL00423695

3.2

Report

- What is the latest position on the Post Office's appetite to corporate Legal & Compliance risks and the minor comment provided by RCC/ARC in 1/2021?
- What are our proposed Next Steps and the timeline?

Background

1. [redacted]

Update

2. Both RCC and ARC whilst formally noting the paper also expressed the view, in advance of formal approval, they were broadly content with the approach and the conclusions reached. They made a small number of comments on which they asked for an update to be provided subsequently. This is the purpose of this paper.

Statutory & Regulatory Obligations (Modern Slavery)

3. [redacted]

4.

5.

Confidential & Legally Privileged

POL00423695

6. [redacted]

Statutory & Regulatory Obligations (Competition Law)

7. [redacted]

8.

9.

10.

Contract & Transaction Management Obligations

11. [redacted]

12.

Key Risk Indicators & Ongoing Monitoring

13. [redacted]

Confidential & Legally Privileged

POL00423695

14. [redacted]

15. [redacted]

16. [redacted]

Next Steps

17. The RCC/ARC are asked to
    - **note** the latest position on the Post Office's appetite to corporate Legal & Compliance risks and our responses to the comment provided by RCC/ARC in 1/2021;
    - **approve** the Legal & Compliance risks appetite position in light of our response; and,
    - **note** proposed Next Steps and the timeline.

Privileged

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

3.3

Title:	Compliance and Audit Report	**Meeting Date:**	16 March 2021
Author:	Jonathan Hill, Director, Compliance Johann Appel:, Head of Internal Audit	**Sponsor:**	Al Cameron, Group Chief Finance Officer Ben Foat, Group General Counsel

Input Sought: Noting & Decision

The Committee is asked to:

1. note the Compliance update.
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

POL00423695

Compliance

Controls Framework

1. Following a decision made by members of the Investment Committee in February, the Controls Project work was stopped, pending a review at the end of the summer.
2. The value of having one master controls framework and IT enabling tool was recognised in the Investment Committee sub-group discussion. Although the approach was to be on a modular, tranche basis, carrying out controls and process mapping in parallel, it was decided that;
   i. The business has enough to focus on now, especially with the Public Inquiry,
   ii. in order to put controls in place, the business first needs to have processes mapped, and
   iii. it needs to have a clear standardised process framework on which to put controls.

Summary of work completed:

3. A Controls Framework was designed together with the user requirements for an operational controls ServiceNow-based system. Deloittes had agreed to review and benchmark the Controls Framework and offer advice on the design and use of the controls tool. This work has been put on hold pending the review in the summer.
4. Recruitment of 3 Controls Analysts to support the project to review, assess and assure the controls identified. The initial scope of work was to capture controls for process improvements that had been put in place following the GLO.
5. It had been assumed there would be process maps in place for each of the business units impacted by the Common Issues judgement ("CIJ") and Horizon Issues judgement ("HIJ"), which the analysts could review for controls. However, few process maps were identified and where they did exist, they were not up to the required standard, with some being out of date.
6. During the period November – December, ahead of a comprehensive Controls tool being built in ServiceNow, a temporary Power Apps workflow tool was developed. This tool would 'house' the controls and allow self-assessment by the business prior to assurance by the analysts. Following testing of the system, a training pack was produced to support the system users.
7. The Business Analysts in the Historical Matters Unit CIJ team started workshops with business units in January; the first being the Branch Reconciliation team (BRT).
8. Further sessions were held with the business areas to gain more information on the controls and provide training on the use of the Power Apps tool.
9. The Controls team also started work with the Postmaster Onboarding Team. An initial review indicated that more work was required to create effective process maps and document controls.
10. As at 19th February, 40 Branch Reconciliation controls had been added to the Power Apps tool and were awaiting assessment by the Controls Analysts.

Telecoms

Data Protection in relation the Telecoms Sale to Shell

11. As part of the Business Purchasing Agreement, Legal, Compliance and IT have engaged with the transaction team to define process for identifying and reviewing data required for BAU activity to continue post-completion. This was agreed on 22nd February and guidance issued to impacted employees. The majority of employees have identified what they require from OneDrive, e-mail and SharePoint. These documents will then be reviewed

Confidential

POL00423695

by DMEs to ensure only information essential for the continuation of the telecoms business is transferred. This is targeted to be completed by 8th March.

12. Compliance is working with the transaction team to establish a post-completion BAU process for management of Subject Access Requests (SARs), including requests regarding personal data for ex-customers of the Telecoms business, for whom Post Office will remain responsible. The transaction team is working with Shell to ensure this process before the completion date of 15th March.
13. During the transaction it was identified that that c5,000 ex-customers were still using a Post Office provided e-mail account. All impacted customers with closed accounts were contacted on 15th February to inform them that their email accounts were expired and that they would be deleted in 28 days' time. The incident and investigation documents have been updated to reflect this closure task
14. Data Sharing Agreement (DSA) – Compliance and Legal are in the process of reviewing and updating the DSA to clarify where Shell and Post Office are acting as Controllers or Processors (or Post Office as a as sub-processor). The DSA is currently with external counsel to make the necessary changes.

Ofcom

15. Communications Incident - There has been no response back from Ofcom yet regarding the comms incident reported in September 2020. Ofcom is reviewing whether it wants to open a formal investigation into the incident and whether to issue a fine. Ofcom is aware of the sale but this may continue post sale should Ofcom decide to open an investigation. If this happens, there are clauses in the contract that require Shell to provide information to Post Office for the purposes of responding to information requests. Meredith Sharples will be available for a short period after the transaction to deal with Ofcom requests but following his departure additional resource may be required to support this.
16. Complaints data – Ofcom will continue to publish the details of Post Office complaints in this year's annual service report because it focuses on historical information. Ofcom has not yet decided when it will remove Post Office from the quarterly complaints reports as the Post Office brand will remain in use post sale for up to 12 months.
17. Information requests – there is one outstanding information request due before the sale completion date, which is on track for successful delivery. If any subsequent requests are received from Ofcom, the contract allows Post Office to request this information from Shell.

FCA

18. PSD2 - The FCA has approved the ECE notification and received the first audit. Further, it has agreed that Post Office can submit its second audit early (covering FY 20/21) and this will be conducted on 8th March.

Data Protection

Data Management – Remote Location / Back Office and Oasis Searches:

19. A project ran in conjunction with Legal, the Historical Matters Unit and Compliance has been progressing since Q3 2020.
20. The objective of this was to provide an assurance to Post Office, our legal team and the Courts that we have conducted reasonable and appropriate searches for any relevant information and have considered any documentation that may be found
21. A review of the boxes identified was completed with all relevant material assessed by the appropriate external law firms for relevance to the various work streams.
22. Any in-scope materials were added to disclosure packs or further analysis was carried out to test for significance to the various workstreams.

Confidential

POL00423695

23. This work is now completed for the Criminal Cases Review Commission (CCRC), the Post-Conviction Disclosure Exercise (PCDE) and Starling. An assessment is to be run for applicability for applicants to the Historical Shortfall Scheme (HSS) with a recommendation due to go the Historical Matters Committee the week commencing 15th March.

Record Retention

24. All Data Owners were identified and provided with a copy of the Retention Schedules, Remediation Logs and copies of the Document Retention and Disposal and Protecting Personal Data policies.
25. The Compliance and CISO teams are starting to work with the business on the remediation logs. There are concerns around the remediation plans and how these can be progressed with initial thoughts that a remediation project may be required.

Record management in branches

26. Compliance, Property Services and the Network team are in the process of standing up a mini-project to implement a change programme for Records Management with the Branches. This project will look to:
27. There are several outstanding issues on this yet, these are:
    - Designing a robust indexing system based on the products and services offered in branch so that we can be sure that the right information is being archived
    - Designing the correct Standard Operating Procedures for the indexing, boxing up and transporting of boxes to Oasis
    - Identifying the best method for transportation of boxes and a decision on where the funding is being provided for associated costs
    - Procuring enough boxes to ensure that we can cover the entire network
    - Developing Comms to go out to PMs on this project.
    - Create a new process for record archiving on a regular basis and not just on the closure of a branch as is the process today
28. Given the demands to complete the Data Management exercise for 22nd February for the CCRC this project is due to start in late Q4 2020-21 or early Q1 2021-22

Post Office Ltd approach to Cookies:

29. As agreed at the January Committee meeting, the DP team is working with the Digital Team in Commercial to determine the commercial impact of making further changes to our cookies approach in order to stay middle of the pack. We are meeting with the Digi Team at the beginning of March to identify a roadmap for how Post Office's solution could evolve over the next 6-12 months.
30. Whilst Post Office continues to remain middle of the pack, as more organisations are changing their approach, Post Office's current position is at risk of falling below the average.
    - We have started to receive external queries with regards to Post Office's implementation of cookies since the last RCC. These queries are in relation to the transparency of our cookie solution and effectiveness.
    - The way in which cookies are implemented in the UK is evolving, with more granular solutions frequently implemented and whilst our solution was good at the time of implementation there is a risk that this will be seen to be less effective as industry's approach changes.

General Data Protection Regulation (GDPR) Contract Remediation

31. 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 is 3 fewer than reported at the previous Committee meeting.

POL00423695

32. We now have an agreed approach on the Fujitsu Horizon Contract and, as part of the Telecoms sale, a signed Data Processing Agreement for Fujitsu Telecoms.
33. Monthly Contract Review Group meetings continue to monitor progress and support negotiations. This will continue until all outstanding contracts are finalised.

Freedom of Information Requests:

34. As a direct result of the GLO, HSS, the public inquiry and having Postmaster seats on the Board we are seeing a change in the number and complexity of Freedom of Information requests.

Freedom of Information Requests (1st September 2020 – 2nd March 2021)

	Historical Matters Related Requests	General Requests	Total Requests
01.09.20 – 02.11.20	12	27	**39**
03.11.20 – 02.03.21	25	35	**60**
Total Requests	**37**	**62**	**99**

35. The more complex cases deal with information which may be either Legally Privileged, Commercially Sensitive, Provided in Confidence or containing Personal Data. There is a balancing act between transparency and protecting Post Office's commercial and legal interests.
36. As a result of this complexity, Legal and Compliance are having to prepare briefs for GE and Board as many of the requests involve sensitive subjects such as the decision by POL to seek to have Justice Fraser recused during the Common Interests hearing.
37. Compliance and Legal meet on a weekly basis with internal and external counsel to ensure that any released information is in line with information released to the Inquiry and to responses made for similar requests by BEIS/UKGI.

Financial Crime

Compliance with Money Laundering Regulations

38. Suspicious Activity Reports (SARs) continue to rise, with 2,955 between 27th October 2020 to 25th February 2021 (compared to 1,074 in the same period last year). The rise is primarily driven by:
    - The continued identification of cases linked to complex banking investigations
    - Branches raising concerns about customers undertaking multiple consecutive high value cash deposits, and
    - Reports from cash centres concerning an increase in branches returning high volumes of Scottish and N.I notes.
    - We also continue to see an increase in suspicious activity from Bureau de Change transaction monitoring despite international travel restrictions and lockdown.
39. In this same period there were 375 Financial Crime investigations (compared to 218 in the same period last year), 38 of these were cash deposit cases (up 65% on 2019/20).
40. We continue to work with the National Economic Crime Centre Project Admiralty and the Banking Framework members to address the risks of cash laundering via Post Office. Cases include:

POL00423695

- Chinese nationals depositing high values onto numerous cards belonging to multiple partner banks at branches located in Scotland advising that the funds are to pay university tuition fees
- c.£7.4m deposited at 9 branches in Birmingham
- Significant cash deposits at c.50 branches in Leicester, which has also been the subject of a Section 7 request submitted by the National Crime Agency (NCA)
- We have also been advised of arrests and cash seizures in relation to some of the Money Service Business (MSB) cash deposits in East London.

41. The risk assessment process was presented at the Commercial lead team meeting in October 2020, and this led to an improvement in stakeholder engagement, however, this has since declined. We are engaging with the product teams to refresh the approach.
42. Payzone - Capita's contract with PIPIT was exited on 31st January and remaining re-seller contracts are being reviewed as part of ongoing Bill Payment and Payzone assessments.
43. The product team is continuing to progress controls for Amazon vouchers, with basket limit controls and pop-up warning being deployed in March, albeit further controls are needed. 39 transactions by 12 customers totalling £27.8k were identified in SAR reports in February, of which c.£11.3k was refused and prevented by branches following targeted training and awareness via Area Managers.
44. As highlighted in the 2021 MLRO report, the accredited Financial Investigations Officer within Security Operations who assisted with the review of SAR disclosures relating to possible Post Office employees and postmasters left the business at short notice in December and the replacement resource will not have the required accreditation. The Financial Crime team are monitoring volumes and assessing resource impact and at the time of writing this report there are a number that are awaiting initial review.

Anti-Bribery and Corruption ("ABC") update

45. An issue was reported in December in relation to a Network employee who received a gift from a customer, which included £60 in cash. This was not identified until after the customer left the branch. The branch was advised to return the funds to the customer but as they have not returned to the branch the branch has been advised to give the cash to charity and provide evidence that this has been done.

Whistleblowing Update

46. Please refer to the separate agenda item.

Fit & Proper (F&P) update

47. Redeclarations for Cohort 1 were completed in good time, with a large number of sole traders completing via the new Branch Hub option. This option is not yet available to limited companies and partnerships, and there is currently not a timescale for delivering this solution. A number of issues were fixed with the release of the changes to accommodate MoneyGram-only and 'paused' branches, but there are still some outstanding issues and a meeting is planned to understand the extent of these and ensure a smooth handover to the new team responsible for agent F&P declarations.
48. Work continues with HR and recruitment to implement better processes for direct employee F&P tests, and there have been no issues in the last 2 months.

External Threats

49. The FCA have started a consultation into Strong Customer Authentication (SCA) and they are exploring the option of increasing the contactless limit from £45 to £100. The risk of increased card fraud has been assessed and it is not believed that this will pose a significant financial crime risk to Post Office.

POL00423695

50. MT Global Limited, a Money Service Business, was fined £23.8 million by HMRC for significant breaches of the regulations between 2017 and 2019. This is the largest ever fine issued by HMRC. The failings related to risk assessments and associated record keeping, policies, controls and procedures. We do not believe Post Office is at risk as the Compliance team carries out risk assessments before product and service go-live and periodically throughout their lifecycle, as stated in the group policy.

Supply Chain Compliance

51. During the remote Supply Chain assurance work at the end of 2020, it was identified that there were issues with the Note Circulation Scheme Bond, with incorrect values being paid in. Subsequently it was established that there were 14 late Bond incidents over the last year. These have now been investigated, root causes established and corrective actions to prevent recurrence have been implemented. Compliance has undertaken assurance reviews at both Birmingham and London to ensure new controls are effective and no further issues were identified. A formal response to the Bank of England was sent on 26th February. The Bank will decide if the incident warrants losing the late Bond facility, issuing a fine or if they take no action.
52. A number of issues were also raised in the remote assurance relating to H&S, many relating to fire door issues. Six are on track to be resolved by end February and the remaining one is likely to be resolved in March, all other fire door issues have been resolved.

Financial Services

Multi Principal Review of 1st line controls.

53. This was reported at the previous meeting. We are still awaiting the first draft of this review from our Principals, we have chased for a response, which is expected within the next 2 weeks.

ATM strategy and Post Office LINK membership.

54. As part of the Post Office strategy of taking over the Bank of Ireland (BoI) ATM estate it has become clear that 2nd and 3rd line oversight needs to be in place for this business activity. In particular LINK membership, which is required as part of this programme, requires control obligations to be met, as ATMs are part of the UK's critical infrastructure and LINK is overseen by the Bank of England.
55. Compliance and Internal Audit are working closely with the 1st line product team through workshops to determine both the type and amount of 2nd line oversight that will be required for both LINK membership but also more widely over our running of the ATM estate.
56. The first milestone will be the end of April 2021 when Post Office will send a draft application to LINK for membership. This will need to include identified controls.

Compliance Monitoring

57. With the implementation of the latest Covid-19 lockdown we agreed with our Principals to suspend branch mystery shopping. Following the Government announcement of the planned easing of restrictions, our mystery shopping company is undertaking a survey of their mystery shoppers to see when they would be willing to commence activity. This is unlikely to be before mid-April and subject to national variations within the UK.
58. Sales of Travel Insurance are currently suspended in branch; all of our other financial services products remain on sale and promotional activity is ongoing for both protection and savings business. As with previous lockdowns, we have been focussing on remote monitoring measures to review performance such as cancelations, complaints and

POL00423695

customer validation calls and regular governance meetings with the Principals remain in place.

FS Key Regulatory updates

59. A summary slide of the key future developments is included in the reading room at Appendix 1.
60. As part of the Government and FCA's focus on access to cash, the FCA is assessing what role it should play in overseeing Post Office as part of this critical cash infrastructure. Nick Read is meeting with the Chief Executive of the FCA to discuss this on 22nd March 2021. In advance of this meeting Ed Smith, the Head of FCA Retail Banking Supervision, has asked for some additional clarity from Post Office in relation to the wide array of financial and related services we provide and their regulatory status. We have provided a response to the FCA with the support of legal and external counsel. Our hope is that this summary information provided will give FCA a rounded view of our services in this area rather than leading into further scrutiny and regulation. This dialogue needs to be managed carefully. Compliance and external counsel are providing advice and a brief for the 22nd March meeting.

Vulnerable Customer FCA Forward Guidance publication in February.

61. The published guidance has followed the lines of the previous vulnerable customer consultations. The FCA expects regulated firms and its Appointed Representatives to ensure the interests of vulnerable customers are protected throughout the product life cycle. There are no new hard rule requirements, but it expects to see firms meet good practice by following the guidance and it has outlined examples of good and poor practice.
62. Post Office has had vulnerable customer on our agenda for some time and we have a number of good practices we put in place, particularly during the pandemic. However, our Principals are undertaking a gap analysis on the guidance to assess if there is anything additional, that they or the Post Office should be doing.
63. The Overall Compliance Dashboards (Appendices 2 and 3) are included in the reading room.

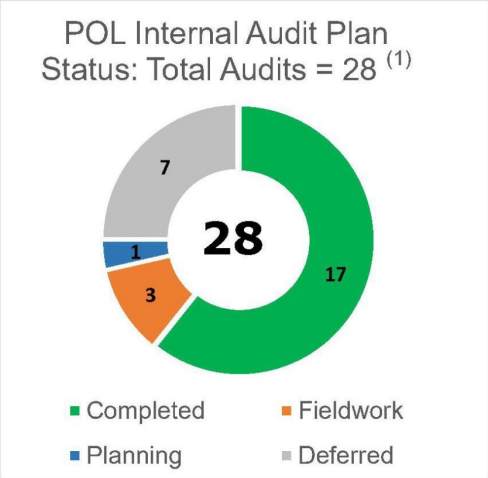
POL00423695

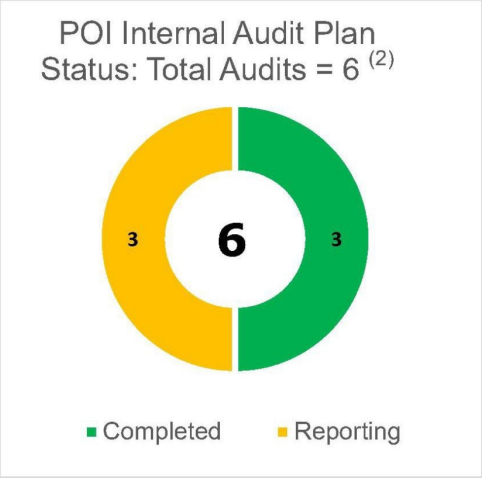
Internal Audit

Progress against Internal Audit plan

64. Delivery of the 2020/21 programme is making good progress, with a further three audits completed in the current reporting cycle.

65. 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 7).
(2)POI ARC approved baseline plan for 2020/21. One additional audit is currently being planned for delivery in Q4/Q1.

66. A re-prioritised Internal Audit programme was approved at the May ARC meeting in response to Covid-19. A more dynamic (quarterly rolling) audit plan was adopted and is being reviewed at each ARC. Further revisions to the plan was approved at the September ARC meeting and is included in the reading room (Appendix 7).

67. An urgent request was received from the GE to support the IDG in assuring all improvements (c.400) in preparation for the Inquiry. Three reviews from the 2020/21 IA plan have been deferred in order to create capacity to support this work.

68. The following audits are in progress or planned for delivery in Q1:

	Review	Sponsor	Timing	Status
1	HIJ Operations Improvement Programme	Declan Salter	Feb	Fieldwork
2	Change Controls Effectiveness	Dan Zinner	Feb-Mar	Fieldwork
3	IDG Support & Assurance - Phase 1 (2020/21 plan)	Dan Zinner	Feb-May	Fieldwork
4	Third Party Revenue Data Assurance	Al Cameron	Feb-Apr	Fieldwork
5	IDG Support & Assurance - Phase 2 (if needed)	Dan Zinner	May-June	Not Started
6	Historical Shortfall Scheme – Claims & Payments	Declan Salter	April	Not Started
7	Note Circulation Scheme (BoE Controls)	Al Cameron	May	Not Started
8	Payzone Control Environment	Owen Woodley	June	Not Started
9	Treasury Operations	Al Cameron	June	Not Started
10	Strategic Platform Modernisation (SPM) Set-up	Zdravko Mladenov	April-May	Not Started

Confidential

POL00423695

Internal Audit reviews completed

69. The following POL audits were completed during the current reporting cycle:

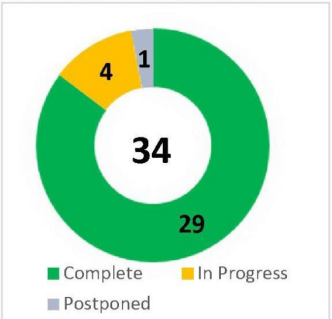
1	Historic Matters – CIJ Improvement Programme (Final Draft Report)	
2	Historic Matters – Set-up & Governance (Final Draft Report)	
3	Postmaster Reporting (Management Information) (Final Draft Report)	

70. Our findings and observations from these reports are summarised below (para. 71-73), with the full reports available in the reading room (appendices 4-6).

71. **Historic Matters – CIJ Operations Improvement Programme** (Ref.2020/21-15)

Not Rated

Progress with completion of NRF recommendations:



Sponsor:
Declan Salter

Audit actions:

P1	5
P2	1
P3	0
Total	6

Appendix 4

Following the judgments from the Group Litigation Order, Post Office has undertaken a programme of improvements to overhaul culture, practices and procedures throughout every part of the business. In addition to launching the Historical Shortfall and Stamps Schemes, as part of its operational improvement plan, and to address issues which arose from group litigation concluded last year, Post Office has established a new Historic Matters business unit (HM) to oversee and deliver the programme of improvements.

Work on formally implementing operational improvements as a result of the CIJ findings has been ongoing since June 2019 and has involved teams from across the whole of POL's operations.

This report is not rated due to the evolutionary nature of the audit work. Our interim report was issued in January 2021 and this has since been adopted as a management tracking tool to drive actions. The Ops Improvement Project was originally planned to have concluded their work in December 2020, but the complications introduced by the OE activity have meant that the project had to be extended until March 2021.

Whilst the remaining actions will not be fully completed until the end of March 2021, there is a clear route to ensure that this deadline is achieved (detailed in the body of the report). A key lesson to be learned by the Ops Improvement Project and HMU is around the need for robust handover processes when passing changes into BAU operations.

Internal Audit will continue to track and validate the remaining actions as part of the assurance provided to IDG in preparation for the Inquiry.

Management Comment

Final draft – comment pending

POL00423695

72. **Historic Matters – Set-up and Governance** (Ref.2020/21-15)

Not Rated (Advisory Review) ***Sponsor:*** *Declan Salter* *Appendix 5*	Following the judgments from the Group Litigation Order, Post Office has undertaken a programme of improvements to overhaul culture, practices and procedures throughout every part of the business. In addition to launching the Historical Shortfall Scheme, as part of its operational improvement plan and to address issues which arose from group litigation concluded last year, Post Office has appointed a new Director, reporting to Tim Parker and Nick Read, to head up a separate business unit responsible to implement the claims schemes and the programme of measures that will oversee the delivery of the operational improvements to address the criticisms from the Common Issues Judgment (CIJ) and the Horizon Issues Judgment (HIJ). Historical Matters Business Unit (HMBU) has been through a period of clarification and refinement of its governance and structure. The design and implementation of the operating model has taken significantly more time and effort than initially anticipated and was initially under-resourced. It has not yet been fully formalised, agreed and embedded. However, this does not mean that HMBU is operating without governance and control. The claimant schemes activities operate within well-defined governance principles supported by the adoption of core 'change' controls since they were launched. As such, key activities could be carried without an overarching HMBU level governance being present. The core 'Change' controls are being phased out, but its transition has not been well structured and clearly articulated. Working in collaboration with HMBU, we have identified areas that require management focus in order to deliver a clear, complete and agreed operational model which must be clearly communicated across Post Office. In addition, we have made suggestions and proposed improvements intended to assist management in their efforts. Although there are key elements pending completion, in our opinion, HMBU is implementing the elements of governance required, although, its pace of delivery must be increased.
Management Comment *Final draft – comment pending*	

Confidential

POL00423695

73. **Postmaster Reporting (Management Information)** (Ref.2020/21-19)



Sponsor:
Amanda Jones

Audit actions:

P1	2
P2	3
P3	1
Total	6

Appendix 6

This audit assessed the provision of management information to Postmasters and the controls in place to ensure that the Postmaster has the means to effectively manage and develop their business. The scope included assessment of data accuracy, integrity & reliability, management information presentation, variation & usability, and ease of accessibility.

We conclude that the provision of management information to Postmasters in its current form, is not fit for purpose. The frequency and quantity of information provided to Postmasters varies depending upon their volume of weekly customer sessions, with all branches categorised according to a three tier system. The area manager structure was revised in April 2019 to ensure every branch receives support. Each area manager is responsible for between 75 and 125 branches of all types and sizes and is the main source of provision of management information for those branches.

The three tier system means that, of necessity, there is a greater priority afforded to the needs of the busier branches, leaving the smaller branches feeling unsupported. There is limited information available to Postmasters on a self-serve basis, largely due to a legacy of under-investment which imposes a significant administrative burden on the area manager population and results in disparity in the frequency that branches receive management information (with smaller (tier 3) branches receiving information as infrequently as once every six months.

Our audit also considered the output from the recent Postmaster consultation, where participants indicated that readily available access to more and improved management information is a priority for the majority of Postmasters. Additionally Internal Audit have directly consulted with Postmasters to understand their perspective and requirements for management information.

Management Comment provided by Amanda Jones (Retail and Franchise Network Director)

"I am pleased that this audit has identified the current limitations we have in being able to provide relevant and timely MI for Postmasters, in a format that works best for them; this finding is consistent with one identified by the current Deloitte review. Having access to key Management Information is critically important to enable Postmasters to operate their Post Offices effectively and for POL to support them to thrive.

The report notes that MI provision of MI is limited due to the variability of Area Manager visits (eg smaller branches receive visits less frequently). Whilst this statement is true, the limitations are largely driven by the lack of MI specifically developed for Postmasters. For example, when an Area Manager visits a branch face to face, they will go through the Branch Insight Tool data with the Postmaster, but aren't able to electronically send it to them, neither is the PM able to self serve. Other reports such as Sales reports, will be emailed to Postmasters if a face to face visit isn't due . This has been the only way to share MI whilst Area Managers have been remote working due periods of lockdown. Therefore it is important to note that whilst it is timely to review the appropriateness of the current branch tiering support model, this in itself will not address the issue of limited MI for Postmasters.

Being able to provide meaningful MI to Postmasters will require input and investment from across business areas. As part of the 'Hot-Housing' programme which started in 2019, a piece of scoping work was completed to determine the MI requirements for Postmasters as-well as the Area Manager. Some progress was made, for example enhancing the Branch Insights Tool. I expect much of this scoping is still relevant so we are not starting from scratch. Successfully addressing the MI requirements for PMs will require appropriate data expertise and systems investment to develop MI in a format that is easy to use and on channels that are easy for PMs to access such as Branch Hub.

Confidential

POL00423695

Post Office Insurance (POI) Audit Programme

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

	Review	Timing	Status / Rating
1	Cyber Security (POL-POI Gap Analysis)	Aug	Satisfactory
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 Dec	Complete (interim report) Fieldwork
4	Special Investigation (Confidential)	Sept	Complete (not rated)
5	Pricing: Principles, policies and process	Nov	Needs Significant Improvement
6	Financial Promotions Communications	Jan	Reporting
7	Effectiveness of Risk Management – original plan	Q4	Planning
8	Channel review: Non-branch sales – original plan		Cancelled (no longer compelling).

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

Status of Audit Actions

75. The movement and ageing of audit actions are shown in the table below (status at 9 March 2021).

Audit Action Status (POL):	
Open actions at last ARC	35
Less: Actions closed in period	16
Add: New actions in period	15
Total open actions	**34**

Ageing:	
Open (not yet due)	33
Overdue (<60 days)	1
Overdue (>60 days)	0
Total open actions	**34**

76. Following is a summary of the overdue action and status update:

Description of audit finding and Priority rating	**GE owner and due date**	**Action Owners and Status Update**
Cyber Security Maturity Assessment (2020)		
Finding (P1): Documentation around current and recommended security architecture is not complete or readily accessible. Action: Document POL's current security architecture and patterns to support POL going forward.	Jeff Smyth Original date: 31/12/2020 Revised date: 28/02/2021	**Owner:** Dave M King An initial draft security architecture document has been received; however further work is required before it can be finalised. Management expects to complete this action by the end of April and progress will be covered in the Cyber Security Update paper.

Confidential

POL00423695

3.3

Appendices[1]

Compliance

Appendix 1: FS Regulatory Calendar
Appendix 2: Compliance Dashboard summary
Appendix 3: Compliance Dashboard

Internal Audit

Appendix 4: Internal Audit Report: Historic Matters – CIJ Improvement Programme (final draft)
Appendix 5: Internal Audit Report: Historic Matters - Set-up and Governance (final draft)
Appendix 6: Internal Audit Report: Postmaster Reporting (Management Information) (final draft)
Appendix 7: Internal Audit Plan for 2020/21

[1] Appendices are accessible in the Diligent Reading Room.

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

4

Title:	2021/22 Internal Audit Plan	**Meeting Date:**	16 March 2021
Author:	Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Finance Officer

Input Sought: Noting & Approval

The Committee is asked to:

- note the draft audit programme for 2021/22;
- consider if the proposed reviews individually and collectively represent an appropriate programme to support management in their activities and to provide assurance to the Audit, Risk & Compliance Committee (ARC) over key risks to Post Office;
- approve the 2021/22 Internal Audit plan, for the onward submission to the ARC.

Previous Governance Oversight

Previous RCC and ARC meeting requests for internal audit reviews have informed the proposed audit programme. Input was also received from GE and Senior Management.

Executive Summary

An integrated audit plan has been prepared to provide assurance over principal business risks and significant change activities. This paper sets out the process followed to identify and select the audit candidates.

The proposed internal audit programme for 2021/22 consists of 24 audits (16 internal control reviews and eight change / programme assurance reviews). In addition, we will also perform around five audits in POI.

Confidential

POL00423695

4

Introduction

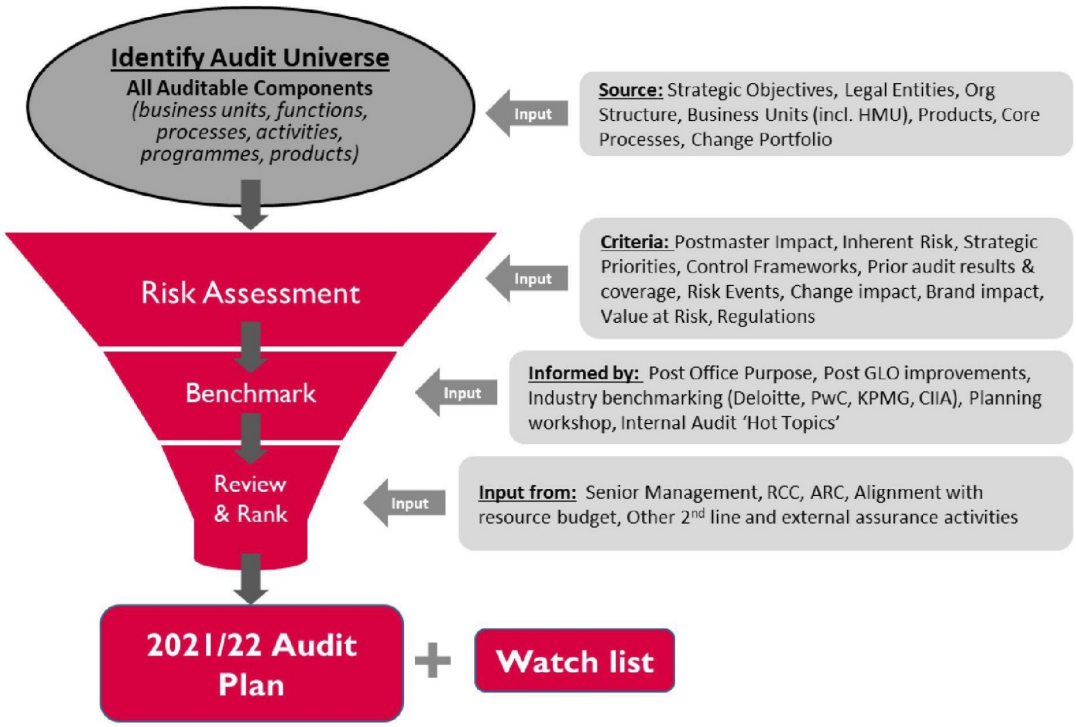
1. The Post Office annual risk-based Internal Audit plan for 2021/22 (2021/22) has been prepared in accordance with the applicable requirements of the Internal Audit Charter as approved by the ARC in May 2020, as well as the professional standards of the Chartered Institute of Internal Auditors (CIIA).
2. The proposed Internal Audit Plan was developed with input from Post Office GE and the wider business, and was benchmarked against industry.

The Planning Context

3. Post Office risk profile is impacted by continued and significant internal change, increased regulatory scrutiny and market pressures. The 2021/22 Internal Audit plan is designed to provide assurance over the organisation's principal risks, core processes and material change activities.
4. The proposed 2021/22 Internal Audit plan is 'Postmaster Centric' and supports the new Purpose and Post GLO improvement activities.
5. In 2017/18 we introduced a three year rotation plan for core processes. Core processes are usually mature and generally expected to be well controlled, but warrant cyclical validation due to their pervasive nature and criticality to the business. The first 3-year rotation was completed in 2019/20; the 2020/21 plan included the start of the second cycle of core process reviews, however, many of the core process reviews had to be delayed in light of Covid-19 priorities. The 3-year rotation plan is therefore being re-assessed and reprioritised. The full three rotation plan is included in para 13.

The Planning Process

6. The following diagram shows the process we followed to identify, assess and prioritise the processes and activities to be assured in 2021/22:



Confidential

POL00423695

The Planning Results

7. The proposed list of audits was discussed and agreed with GE members and senior management and their feedback has been incorporated.

8. The tables below outline the proposed internal audits to take place in 2021/22. Internal and external events may cause priorities and risk profiles to change, and management may have additional requests during the year for advisory support or audit assistance. In consequence, we may consider amending the plan as the year progresses. We will also re-assess and refresh the plan at least quarterly to ensure it remains relevant. We will seek ARC approval for all material changes to the plan.

9. Table 1 represents the baseline plan for internal control reviews, including reviews of the Historic Matters Unit and Post GLO improvement activities. The target delivery is 16 reviews. High level audit scopes for each review can be found in Appendix 1.

Table 1: Internal Control Reviews (target = 16 reviews)				
Rank	Proposed Review	GE Sponsor(s)	Postmaster Impact?	Timing
Priority Audits				
1	IDG Support & Assurance - Phase 2	Dan Zinner	Direct	Q1
2	GLO Historical Shortfall Scheme – Claims & Payments	Declan Salter	Direct	Q1
3	Note Circulation Scheme (BoE Controls)	Al Cameron	No	Q1
4	IDG Support & Assurance - Phase 3	Dan Zinner	Direct	Q2
5	GLO Stamp Stock Scheme	Declan Salter	Direct	Q2
Rolling Plan				
6	Payzone Control Environment	Owen Woodley	No	Q1
7	Treasury Operations	Al Cameron	Indirect	Q1
8	Effectiveness of Second Line – Financial Crime Function	Ben Foat	Indirect	Q2
9	CFS Application Controls	Al Cameron	No	Q2
10	Effectiveness of Compliance Function	Ben Foat	Indirect	Q2
11	JML Deep Dive	Jeff Smyth	Indirect	Q3
12	IT Operations and Incident Management	Jeff Smyth	Indirect	Q3
13	Cyber Security Maturity	Jeff Smyth	Indirect	Q3
14	ATM Link Scheme Assurance	Owen Woodley	No	Q4
15	Third Party Data Validation	Al Cameron	Indirect	Q4
16	Business Continuity (Incl. Post-crisis assessment and ITDR)	Al Cameron	Direct	Q4

Confidential

POL00423695

10. Table 2 below shows a list of reviews with a Postmaster Focus. We expect that many of these processes will be covered through our IDG assurance work. We will assess the need for end-to-end reviews of these areas based on the outcome of the IDG assurance work and the Inquiry.

Table 2: Alternative reviews with a Postmaster Focus			
Rank	Proposed Review	GE Sponsor(s)	Postmaster Impact?
1	Horizon Application Controls (follow up KPMG recommendations)	Jeff Smyth (Simon Oldnall)	Direct
2	Postmaster Journey Follow-up (Placeholder)	Amanda Jones	Direct
3	Postmaster Performance Management & Offboarding	Amanda Jones	Direct
4	Postmaster Issue Resolution	Amanda Jones	Direct
5	Revenue Protection (Deep Dive)	Dan Zinner	Direct
6	Postmaster On-boarding Process	Dan Zinner	Direct
7	Branch Cash Forecasting	Al Cameron	Direct
8	TransTrack Application Controls	Russell Hancock	Direct
9	Stamp Stock Controls	Al Cameron	Direct

11. Table 3 represents assurance provided over Post Office's change risk. The baseline plan is for eight change assurance reviews. This is an indicative list based on the current change portfolio and will be reviewed and updated continuously as the portfolio of change programmes develop and the risk profile changes.

Table 3: Programme Assurance (target = 8 reviews)				
	Proposed Review	GE Sponsor	Postmaster Impact?	Timing
1	Strategic Platform Modernisation (SPM) Setup	Zdravko Mladenov	Direct	Q1
2	Belfast Follow-up	Jeff Smyth	Direct	Q1/2
3	PCI Follow-up - Part 2	Jeff Smyth	Direct	Q2
4	SPM Mobilisation/Delivery	Jeff Smyth	Direct	Q3/4
5	Change Controls effectiveness	Dan Zinner	No	Q4
6	Belfast Follow-up - Part 3	Jeff Smyth	Direct	Q3/4
7	Placeholder Change Project (TBC)	TBC	tbd	TBC
8	Placeholder Change Project (TBC)	TBC	tbd	TBC

Confidential

POL00423695

12. Table 4 is our 'watch list' of alternative topics and additional areas for consideration during the year, should either the assurance needs for the priority areas decrease or risk levels for items on our watch list increase. The watch list will also inform the 2022/23 internal audit plan.

Table 4: Watch list alternative topics (top 10 items only)	
	Topic / Area
1	ITCF Follow up
2	Financial Controls Framework
3	Management of Strategic Partners
4	Compliance with Prompt Payment Regulations
5	Product Risk Assessment (MoneyGram / Lottery Products / ATMs)
6	Top Down / Overarching People Review / Onboarding Process
7	ServiceNow Implementation
8	IT DR (Deep Dive After Belfast Exit – Q4/2021/22)
9	Effectiveness of IT Security - Operational (2nd Line)
10	Management Information (Fit for purpose / standardised / one version of truth)

Three Year Rotation Plan

13. We introduced a rotational audit plan in 2017/18 to assess core business processes over a three year cycle in order to provide regular assurance on the effective operation of controls over critical business processes. The rotational plan in the table below has been based on the last review of these processes, known issues and ongoing remedial programmes.

Core Processes – 3 Year Rotation Plan		
Year 1: 2021/22	**Year 2: 2022/23**	**Year 3: 2023/24**
Financial Reporting Controls N2	Financial Reporting Controls	Financial Reporting Controls
Third Party Data Validation N1	Third Party Data Validation	Third Party Data Validation
Contract Management (Strategic Partners) N2	Sales (Product tbc)	Supply Chain Management (CViT)
Branch Cash Forecasting N2	Payroll	Employee Expenses
Business Continuity N1	Financial Close Process	Agents Remuneration
IT Operations N1	Fixed Assets	FS Conduct Management
Cyber Security N1	Procure to Pay	Bill to Cash (Accounts Receivable)
Treasury Operations N1	Client Settlements Process	Sales (Product tbc)
Regulatory Compliance N2		

N1 – Included in 2021/22 rolling plan. N2 – To be prioritised once other priority audits have been completed.

Confidential

POL00423695

Post Office Insurance Internal Audit Plan

14. We will carry out a programme of internal audit reviews on behalf of Post Office Insurance (POI), as per the Master Service Agreement between POL and POI. The 2021/22 plan is pending approval by the POI ARC, and will be reported to the POL RCC and ARC once this is done.

Financial Impact

15. The approved headcount for the internal audit team is 6 FTEs. We are currently at full headcount. The co-source requirement to support delivery of the 2021/22 plan was estimated at approximately 470 days with a total cost of £523k (excluding POI).

16. The cost implications of the co-source element of delivering the internal audit plan is as follows:

Category	Number of audits	Estimated effort (days)		Co-source cost	
		Total	Co-source	2021/22	2020/21
Core Internal Audit	16	610	255	£255k	£240k
Change Portfolio	8	375	215	£268k [N2]	£191k
Total	**24** [N1]	**985**	**470**	**£523k**	**£431k**

[N1] 2020/21 plan was for 26 audits.

[N2] The increase in forecasted cost for change assurance is to provide for SME input into complex programmes, such as Belfast Exit, SPM and PCI.

17. During 2018/19, we benchmarked the cost of providing Post Office internal audit services against Deloitte's 2018 Global Auditing Information Network (GAIN) Survey. Post Office spends around 0.14% of revenue on internal audit, which was found to be comparable with similar size FS organisations (0.12%) and higher than similar size retail organisations (0.04%). We believe that the level of spend on internal audit is appropriate for the nature and size of the organisation and that this benchmark is still relevant.

POL00423695

Appendix 1 - High level audit scope statements

Rank	Proposed Review	High Level Scope
1	IDG Support & Assurance - Phase 2	To provide independent validation and assurance over key improvements in support of the Inquiry. Around 400 improvements have already been identified, which will be validated for completeness and effectiveness. Testing will prioritise highest Postmaster impact actions and will be proportionate to the risk.
2	GLO Historical Shortfall Scheme – Claims & Payments	Review of the scheme governance arrangements, including oversight, reporting, escalation and claimant journey. Review of operational controls to ensure the prompt and proper resolution of claims.
3	Note Circulation Scheme (BoE Controls)	Review the controls over BoE notes held in vaults, the process of moving notes to 'borrow' from BoE and accuracy of declaration to BoE and accounting treatment.
4	IDG Support & Assurance - Phase 3	Same as item 1. This is a placeholder to validate additional improvement in preparation of the Inquiry or as a result of the Inquiry.
5	GLO Stamp Stock Scheme	Review of rationale, set up and controls of the scheme, including controls over the logging, assessment and payment of claims.
6	Payzone Control Environment	To include compliance with POL Group Policies and progress to bring IT systems, equipment, security and resilience up to an acceptable standard.
7	Treasury Operations	Assess the design and operating effectiveness of end to end Treasury operations, including Governance, Policies & Procedures, Skills & Capabilities, SOD, bank mandates, & DOA.
8	Effectiveness of Financial Crime Function	Review of Financial Crime function activities, to include team resilience. Will consider both first and second line activities, and clear separation between the lines.
9	CFS Application Controls	Review general application controls including OS, Database and application access, system and change control, IT operations and DR.

Confidential

POL00423695

Rank	Proposed Review	High Level Scope
10	Effectiveness of Compliance Function	Review of scope vs. expectations across business, particularly of the interaction between first and second line activities and the split between compliance and the first line.
11	JML Deep Dive	Review status of JML roadmap, in-depth testing of joiners, movers, leavers, PAM, RBAC, SoD and re-certification. Review integration/automation, etc.
12	IT Operations and Incident Management	Provide assurance that IT services are delivered consistently, reliably and at an appropriate level of service. This includes management of infrastructure changes, monitoring of operational IT infrastructure, and issue diagnosis and resolution. The backup and recovery of systems in the event of an incident or service interruption is covered separately under IT DR (incl. in Business Continuity).
13	Cyber Security (Maturity Assessment)	Assess the implementation of the agreed actions and evaluate the level of progress towards increased Cyber Security Maturity following the 2019 and 2020 Deloitte assessments. Progress will be assessed across the highest risk domains and those areas highlighted by the 2020 review to be in most need of improvement.
14	ATM Link Scheme Assurance	Following the takeover of ATMs from BoI, Post Office need to join the Link Scheme, which has a requirement for annual attestation by the 3rd line that the Link Scheme controls were complied with.
15	Third Party Data Validation	Review Business Process and IT controls for key revenue generating third parties to ensure accuracy, reliability and integrity of data. Perform data analytics as necessary.
16	Business Continuity (Incl. Post-crisis assessment and ITDR)	To assess how the learnings from the business response to Covid-19 have been embedded in BC management. To include a review of overall BCP processes and focus on ITDR for Horizon.

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE REPORT

Title:	PCI DSS Compliance	**Meeting Date:**	16 March 2021
Author:	Patrick Juan, PCI DSS Programme Manager	**Sponsor:**	Jeff Smyth, Group Chief Information Officer

5.1

Input Sought: Noting

The Committee is asked to note:

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

Previous Governance Oversight

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

Executive Summary

The PCI programme has made good progress in several key technical areas, with various milestones having been completed. However, at the time of submission there are two main areas for concern that the programme team is working through. The first is an unexpected delay on Fujitsu exit of SV&I that impacts project delivery by 3 weeks. The second is impact of resources contention at Fujitsu: various demands on Fujitsu resources impact the programme significantly, e.g. Cash Management pilot on 5 branches impacting PCI Programme potentially by an additional 4 to 6 weeks.

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.

Retail Payments Pilot: During the last period the pilot has completed successfully. Lessons learned exercise conducted and major issues corrected in subsequent release to be delivered once branches are rolled out.

Banking development: During the last period, significant progress has been made by Ingenico. Their delivery has passed Vocalink pre-accreditation and is about to complete full accreditation with confirmation of pass expected imminently at the time of writing. However, the Pilot for Retail Payment and Banking transactions is being delayed by Fujitsu SV&I activities reporting higher volume of defects than expected. This adds a 3-week delay on pilot date (24/5 latest expected date of pilot start).

Confidential

POL00423695

The Target Operating Model workstream is progressing well. Discussion with Santander has progressed and we now have confirmed early July delivery. This will extend the pilot. Project activities with First Rate (FRES) to make TMC PCI-compliant have started. Bank of Ireland (Release I) has agreed to change the deposit limit to £10k to support BIN >6 product harmonisation significantly de-risking the delivery.

Risk of further Costs

A risk that further costs might be incurred was highlighted at the last report. Since then, the PCI Programme has identified and estimated the cost uncertainties and it is in the process of requesting a £4.1M drawdown for new funds for the programme. It has been approved by IC and is to be submitted at the next POL Board meeting. An additional £3M of known risks and further contingency that may need further funding has been also approved.

Questions addressed

1. What has been the progress since the programme last presented in January 2021?
2. What are the key risks and issues on the programme?

Report

1. What has been the progress since the programme last presented in January 2021?

Summary of key achievements in the last period:

- The **Retail Payments pilot** completed successfully at 5 branches with end to end payment process from acceptance to reconciliation with Global Payments validated.
- **Banking transactions:**
  - SV&I activities started but delayed due to extra complexity and high level of issues being corrected
  - Ingenico Vocalink ready software has gone through pre-accreditation successfully and is about to complete full accreditation with Vocalink (week starting 15/03).
  - Agreement with banks regarding institution ID making the switch to Ingenico solution transparent from a processing perspective de-risking significantly dependencies on banks readiness.
  - Monthly communication to Banking Framework well received.

- **Target Operating Model (TOM):**
  - **Santander:** Confirmed delivery for 5th July. Impact will be an extended pilot.
  - **TMC:** FRES has initiated project activities and team has commenced work.
  - **Bank of Ireland:** BOI agreed to change the deposit limit to £10k to support BIN >6 product harmonisation.
  - **CDE:** Development completed.
  - **Commercials:** Finalisation of contracts for PAN key entry, reference data changes, BIN>6 development, PODG scanning and testing.
  - **Communications:** Branch Focus comms were released for remediation of branch forms and receipts

- **PCI DSS Audit**
  - Confirmed approach to pre-audit activities with QSA. Central pre-audit scheduled for w/c 26 April.
  - Full audit planning discussion with QSA starting.

POL00423695

- **Pivot to Cloud.** Working closely with the Pivot to Cloud team to manage dependencies due to overlapping timescales.

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

The following are identified as key risks:

Risk: High risk on delivery timeline slipping due to Fujitsu/Ingenico delays. Recent delays in SV&I at Fujitsu have introduced a 3-week delay pushing back start of Model Office to 17 May. Refer to Appendix 1 for latest timelines.
Mitigation: Weekly reviews with Fujitsu to identify remediation paths wherever possible and to ensure no further slippage.

Risk: High risk of delivery time slipping due to Fujitsu resource contention. Fujitsu is being asked to perform other activities at short notice without consideration of impact on PCI Programme, e.g. Cash management pilot at 5 branches impacting PCI Programme by 4 to 6 weeks. This may also impact BEX programme similarly.
Mitigation: Ongoing review with Fujitsu to look at any options to remove risk on PCI Programme. However, priorities to balance business needs and major transformation programmes must be established at POL.

Risk: Due to the complexity of the solution further funds will be needed. Fujitsu is forecasting an overspend; further funds will also be needed to accommodate the change in delivery approach. The contract is T&M and there is a risk of further overspend.
Mitigation: Post Office has challenged the forecast overspend with Fujitsu and will continue to track and manage this issue. Further funding will be needed.
Mar 21 update: Additional drawdown of £4.1M is being processed. IC review on 8th March has been approved and is to be presented at next Board session. An additional £3M of known risks and contingency that may need further funding has been also approved.

Refer to Appendices 2 and 3 for more details on financial summary and IC submission.

Update on other risks reported in January 21 report

Risk: There is a high risk that Santander cannot migrate services to route through Vocalink within the timescales required and this will significantly affect the programme.
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 and escalation meetings are taking place. Jan 21 update: Santander is indicating that they cannot implement the required change until Q3/2021. A director level meeting is scheduled for the first week of January to see if this delay can be mitigated.
Mar 21 update: Santander has provided first version of plan that indicates delivery early July. This will have an impact on branch pilot as this delivery is a must have but other risks on overall delivery timeline (see above) may lessen the impact of Santander delivery.

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.

POL00423695

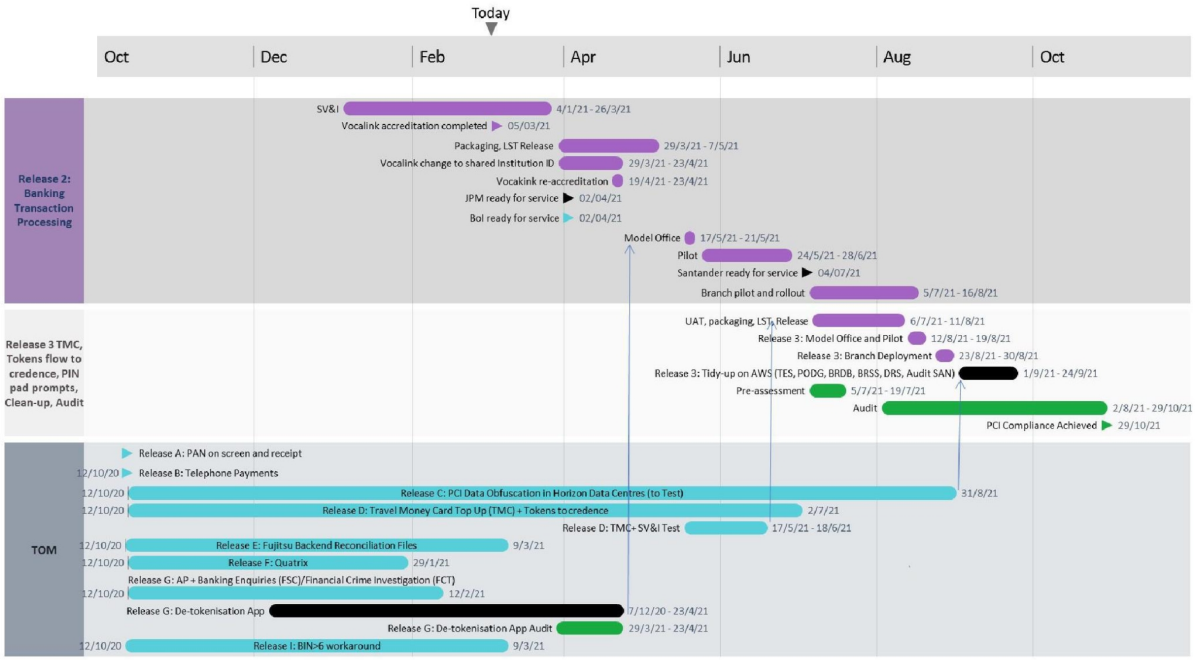
Mitigation: Post Office has managed to descope some of the changes identified by working with the business. At steerco it was agreed to implement two of the essential changes – BIN>6 processing workaround and Ingenico tokenisation. TMC could not be accommodated and so this will be delivered as a separate 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.
Mar 21 update: Agreement with FRES to deliver TMC functionality as part of a subsequent release (release 3 tracking towards 23/8/21 for Branch deployment). Refer to Appendix 1 for current timelines.

Risk: Bank of Ireland / Instant Saver. Due to the limitation in the Ingenico product to be able to process BIN ranges greater than 6 digits we have had to ask Bank of Ireland to implement a £10k deposit limit in their systems. There is a high risk that it cannot implement this within our timescales which would delay the overall programme.
Mitigation: Post Office is working with BoI/IS to plan the migration. Early information indicates that their development may not be complete until June 2021 at the earliest which would directly impact the plan
Mar 21 update:
BOI has agreed to harmonise BOI card products on same BIN range as Instant Saver to match the £10k deposit limit. On track to meet BIN 6 delivery requirements.

Confidential

POL00423695

Appendix 1: Programme plan – Current plan with built-in delays from various activities, not including Fujitsu resource contention risk



Confidential

POL00423695

Appendix 2 Finance Summary

The latest forecast below was presented to the Investment Committee on 8th March.

PCI Programme Capex & Exceptional Spend (2018-2022)	Spend (to end Mar '20)	2020/21 Actual+F/Cast (Apr'20-Mar'21)	F/Cast 2021/22	LIFE
Internal Labour	£142,589	£598,191	£260,821	£1,001,600
External Labour	£1,016,232	£490,917	£541,375	£2,048,524
3rd Party Costs	£3,727,554	£8,548,733	£4,431,145	£16,707,432
Exceptional Costs	£115,000	£0	£0	£115,000
Actual / Forecast	**£5,001,374**	**£9,637,841**	**£5,233,341**	**£19,872,556**

Confidential

POL00423695

Appendix 3 IC Submission of additional drawdown and cost risks details

IC submission summary.

PRJ0010421 – PCI Programme

Decisions

1. Funding: IC to approve an increase in funding of £4.1m that will be presented to Board.
2. Drawdown: IC to approve drawdown of the new funds of £4.1m.
3. Risk: IC to note that £1.1m of known risks may need further funding if they crystallize. We will request Board to allow IC to authorise these funds if needed. In the interest of transparency new risks may be identified that may lead to further cost risks.
4. Interim approval: There is a risk that the programme will exceed the 2% limit prior to completion of the Board approval process. The programme is asking for interim approval of £423k to cover Ingenico costs to allow the programme to raise an urgent PO to avoid programme delays.
5. OPEX: IC also requested to approve supporting BAU OPEX charges (next slide).

Background / Commentary

1. Programme is making good progress and has delivered a working Ingenico Payments pilot to five branches.
2. Board approved £15.765m Business Case in May 2020.
3. Current forecasts indicate the programme needs £19.9m.
4. Some uncertainty in costs remain as work is still being commissioned – currently indicated at a further £1.1m.
5. Risk of one specific dependency (Santander readiness) delaying the programme and causing further costs.

Confidential

POL00423695

The table below shows the breakdown of the £1,104K of identified known risks with their associated risk profile.

Workstream	Costs description	Jan '21 Forecast (£)	Upper Limit	Certainty (%)	Opportunity /Risk (£)	Commentary
IT/TOM	Actuals (to Jan '21)	13,108	13,108	100	0	These are the costs to date.
IT/TOM	Costs where PO raised and understood (Resource, Vocalink,...)	1,104	1,115	99	11	These costs are well understood but there is a small risk of an overspend.
IT	Release 2 & 3 Non Fujitsu Costs (Counter Training, Testing, Packaging, POCA Card Assoc., SCA)	455	682	50	227	Some forecast costs are estimated, there is a risk that we may need further CC packaging or testing resource. There is also a risk that additional functionality may be required such as Counter Training or SCA.
IT	Release 2 (Remaining Fujitsu & Ingenico Costs incl. PIN Pad activation costs)	2,422	2,664	90	242	Fujitsu forecast T&M costs have been increasing. There is a risk of further increases from Fujitsu and Ingenico.
IT	Release 2: Santander Budget Provision	187	243	70	56	Santander are still scoping out the changes needed and there is a risk these costs will be higher than provisioned. We expect the Santander costs to be confirmed mid-Feb 2021.
IT	Release 3 (Fujitsu and Ingenico Costs)	362	398	90	36	There is a risk that the T&M costs for Release 3 may increase due to further unexpected complexity or longer delivery timelines.
IT	Release 3 Additional Resources to cover the new TMC release (FRES may seek some compensation charge for the remediation) and Fujitsu / POL delays (Jul to Dec '21)	947	1,041	90	95	Forecast resource costs are aligned with the latest programme plan and allow time for PCI accreditation to complete and project closure however there is a risk of further programme delay resulting in additional costs.
Programme	Strengthening the Programme Team (Atos) to June '21	0	0	99	0	We have fully allocated ATOS resources to the end of June 2021. ATOS provide very experienced /competent resources. The ATOS exit is introducing a risk to the programme in terms of quality and timescales (at least 1-2 months). Mitigation steps are being put in place with replacement contract staff. This is likely to significantly impact the programme timeline and quality. A small reserve of £35k would cover some handover.
TOM	TOM Release C: Clean Up	945	1,228	70	283	Sixteen systems have been identified for Obfuscation / clean-up of data. We have started the quotation process for some of these systems and work is ongoing to obtain firm pricing. This clean-up activity is not needed until Q3/2021. We anticipate that firm costs will be available in May 2021. There is a risk that the firm pricing will exceed the budget allocated.
TOM	TOM Release F + G: (Clean Room, Mimecast) and Legal Services and Nettitude Audit)	249	373	50	124	There is a risk that further clean room costs may be needed to complete the delivery.
TOM	TOM Release I: BIN>6 Workaround to Ingenico Solution (incl Bank of Ireland CR)	95	123	70	28	We have a solution identified for the BIN>6 work. There is a risk that we may need to fund some BoI change to accommodate this BIN>6 change.
		19,873	**20,976**		**1,104**	

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Cyber Security Update	**Meeting Date:**	16 March 2021
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Group CIO

5.2

Input Sought: Noting

The Committee is asked to note the status and plans regarding the reduction of risk associated with Cyber Security.

Previous Governance Oversight

Rolling item at each Committee.

Executive Summary

- We continue with our programme of work to develop higher levels of cyber maturity. Progress continues on track in all areas.
- We describe the focus of our 21/22 programme balancing the needs for focus on inquiry, postmasters and cyber maturity increase.
- We describe the results from our second desktop cyber incident drill.
- Our current cyber operations dashboard and resulting highlights are discussed.

Questions addressed

1. What is the latest update on the cyber programme?
2. What is the focus of our 21/22 cyber programme?
3. What are the results from the recent cyber incident desktop drill?
4. What are the highlights from the current Cyber Operations dashboard?

Confidential

POL00423695

Report: Programme Update

1. 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	**Completed –** approved by GE	30/11/20
Security architecture is not fully documented	**In progress –** first draft requires further edits	28/2/21 revised date
There is no documented long-term cyber strategy	**Completed** – next update Q2 2021	31/12/20
There is no end-to-end programme defined for Cyber	**In Progress** – being developed in line with 21/22 planning cycle – programme focus discussed in this paper	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	**Completed**	28/2/21 revised date

2. The roadmap for the cyber programme and dependencies is described in the next section.

Report : What is the focus of our 21/22 cyber programme?

3. Since we planned our 2020/21 programme the world of the Post Office has changed significantly. As per the above table we have developed a new cyber strategy which we have adapted to focus on three themes:
    a. **Postmaster support**
        i. **Activities that directly support postmasters** which will cover but not be limited to hardening of counter terminals, detection/prevention of external fraud against postmasters, fraud detection within the network and rationalisation of access management controls.
        ii. **Indirect postmaster support** – through providing cyber input to key programmes that are aimed at keeping postmasters at the centre of what we do e.g., SPM, PCIDSS, Banking Framework
    b. **Inquiry-related improvements** – resulting from the CIJ, HIJ and other inquiry-related activity
    c. **Group-wide Cyber maturity increases** – those activities that reduce the overall risk to the whole organisation and help ensure that the Post Office exists/is not taken out for a significant amount of time. The Group functions cannot exist without postmasters and vice versa. These improvements are aimed at us reaching our cyber maturity targets.

Confidential

POL00423695

4. A one-page view of the programme is at Appendix 1.

5. The programme is now going through portfolio and financial approval.

Report : What are the results from the recent cyber incident desktop drill?

6. We previously reported to the committee that, whilst we had confidence in our defences, we were keen to perform a number of desktop incident drills. We have recently completed the second of these and this is described below.

7. We engaged Nettitude (our red team and pen test supplier) to run the test for us using skilled personnel to simulate potential large-scale loss of customer data.

8. The test was designed to be as realistic as possible and was run remotely due to COVID restrictions. The following constraints applied:
    a. No malicious code was to be introduced by Nettitude during the incident.
    b. Any PII data used during the exercise was fake and randomly generated.
    c. Nettitude would not provide any 3rd party Incident Response resources – we could only use our own and other third party if we had them.

9. The scenario we tested was as follows:
    a. You have this morning received communication from a freelance security researcher at email address stumpyuk1@ GRO , sent via the "Contact Us" web form on the Post Office website.
    b. The researcher claims to have found some interesting data on the internet: An individual who posted the data on the paste site claims to be in possession of full dump of customer data from the Post Office.
    c. The researcher has sent you 3 x sample of records. The security researcher has copied and pasted the message in his message to the Post Office.

10. During the exercise a number of interruptions were made by Nettitude as the incident progressed with new and emerging facts.
    a. **Inject 1** - You are unable to find the claimed information online. After communication with the security researcher, he enquires if Post Office offer a bug bounty and if so suggests 0.1 BTC might be a suitable bounty to pay in return for the URL to the paste site.
    b. **Inject 2** - The Post Office may pay the bounty or convince the researcher to supply the URL (or completely disengage with the researcher). If more interaction with researcher, they send the URL to the paste.
    c. **Inject 3** - The Post Office confirm that the 2x samples are consistent with data that they hold. The samples claim to come from The Post Office and the paster has provided an email address and demand for 0.1BTC for full copy of the dump. Researcher eventually discloses the URL:Pastebin.com/VEBjcYBB

Confidential

POL00423695

d. **Inject 4** - Multiple Post Office customers contact The Post Office claiming that they have received phishing emails that contain specific and accurate information only held by the Post Office.

11. The results of the test are discussed below – taken directly from the Nettitude report with no edits.

12. The scenario presented to the Post Office was complex and contained uncertainties along with issues that cut across multiple departments. As such, representatives from the Cyber Security Team, Major Incident Management Team and Data Protection Team were involved in the exercise.

13. In terms of ***People***, The Post Office staff performed to a very high standard during the exercise. They were presented with a wide range of complex issues and they were quickly able to identify the risks and develop strategies for managing the risk. They closely followed the processes documented in relevant policies. Each of the relevant stakeholders demonstrated that they had an excellent grasp of the documented policies that they were responsible for. The decision making, based on available information was also excellent. All the representatives on the exercise pooled their knowledge in order to work their way through an increasingly complex set of problems.

14. In terms of ***Process***, during the exercise, documented processes were tested to their limits and withstood complex issues that progressively escalated in severity. It was apparent to Nettitude that a lot of thought and planning had gone into the development of the documents. As the scenario progressed The Post Office correctly escalated their response at the appropriate junctures, and seamlessly handed off ownership to the correct stakeholders. In the previous tabletop exercise delivered to the Cyber Security Team, gaps were found in the documented Cyber Security Incident Response processes. Those gaps have now been closed, thus during the initial phase of the incident, the incident was correctly categorised and subsequently correctly escalated into the Major Incident Management Team. The participants in the exercise were able to identify which team had overall ownership of the incident during its progress and were able to identify the correct organisations and Post Office stakeholders to notify at the correct time.

15. In terms of ***Technology***, In respect of this specific incident, it was noted that whilst The Post Office have strong policies in place around how Personal Information is stored and shared, they have no technical solution for locating Personal Information within their network, thus ensuring that Data Protection policies are being adhered to. Within the scenario presented to them, The Post Office identified the need to establish where within their network that customer Personal Data was held, they had no technical means to achieve this. In addition, the identification, procurement, and deployment of such a solution would likely take weeks or months, thus be of limited value to The Post Office. Nettitude's experience is that quickly deploying data discovery tools to scan a network of The Post Office's size would cost upwards of £1.5 million pounds. The Post Office should therefore assess the impact of a large-scale breach of their customer data and consider if there is value in purchasing a data more reasonably priced solution ahead of any such potential event.

Confidential

POL00423695

16. In summary
    a. The Post Office Cyber Security, Major Incident and Data Protection staff successfully completed the tabletop exercise.
    b. Gaps previously identified in the Post Office's Cyber Security Incident Response documentation were confirmed to have been closed.
    c. No gaps were found in respect of the Post Offices current documentation for managing security incidents.
    d. Gaps were found in The Post Office's technical capabilities to quickly identify the location of Personal Information within their network. The need for this capability will be assessed as part of programme planning for FY21/22

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

17. Appendix 2 shows the current cyber operational metrics dashboard.

18. Key points to note:
    a. Controls maturity increases have slowed due to focus and funding being applied to inquiry and postmaster activities.
    b. We have completed the insource of our Security Operations Centre (SOC) from Verizon at a net annual saving of £450k.
    c. There is an increase of activity around managing security of our 3rd parties with particular emphasis on Fujitsu but with broader application to follow.
    d. We completed the follow up with GE members on the recent fake phishing attack. Those who clicked on the link but did not complete the follow up 5 minute training task have been individually contacted by the relevant GE members.

Confidential

POL00423695

Appendix 1 Cyber 21/22 Programme & Alignment with Priorities

Item	Description	Alignment		
		Inquiry	Postmasters	Cyber Maturity
Security Incident and Event Monitoring (SIEM) enhancement	• Expand our capability to cover PO Group plus Horizon. • Expand our capability to cover Office 365 and AWS by integrating their native tools with ours • Expand to cover fraud and branch network monitoring	★	★	★
Data Loss Prevention	• Build capability to block personally and commercially sensitive data leaving the organisation	★	★	★
Service Now Integration	• Delivery of modules to provide integrated incident ticketing, risk assessments and IT controls against Post Office asset database		★	★
User authentication	• Delivery of a password management tool to help users store and retain complex passwords across the POL Estate • Delivery of Multi-Factor Authentication capability to reduce the risk of unauthorised access	★	★	★
Outbound Email security	• Use of DMARC/DKIM technology to stop spoofing of emails to customers and postmasters	★	★	★
Device authentication	• Deployment of Network Access Control to stop unauthorised devices connecting to the Post Office network – corporate and retail	★	★	★
Reviews and Red Teams	• Real-life friendly hacking of our defences to enable hardening • Benchmark and maturity assessments of all cyber defences vs Deloitte Standard		☆	★
Forensics	• Re use of capability developed by GLO team to become persistent and POL Group-wide		☆	★
IAM/JML	• Automation of HR/IT JML processes to reduce risks associated with JML	★		★
Postmaster Security	• Hardening of the counter terminals • Detection/prevention of fraud against postmasters – • Fraud detection within the network • Rationalisation of access management controls	★	★	☆
Cyber Behaviours	• Develop capability and tooling to produce interventions and measure change in people's behaviours around cyber and data protection		★	★
Cyber Risk	• Representation of Cyber risk in monetary terms • If a ransomware attack happened to POL, what would be the impact ££££			☆

Confidential

POL00423695

Appendix 2 Cyber Dashboard

Cyber Operations 1

Threat Landscape (Cyber Perspective)

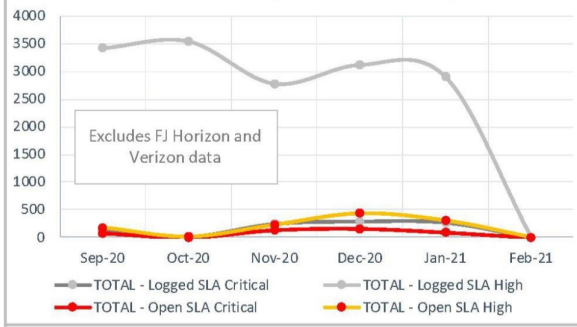


Overall Security Posture

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

Little to no maturity gain as the cadence of change slows, pressures on funding and operational demands from GLO. Small increases in Maturity in coming months as alert use cases in SIEM tooling now under SOC control are developed at pace. Additional load to SOC due in April with onboarding of PCI to scope. Centralised Vulnerability management via ServiceNow ITSM tooling will bring enhanced intelligence to view.

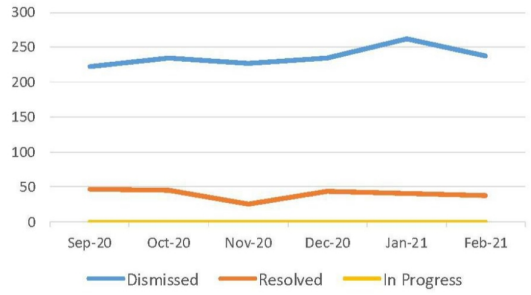
Vulnerabilities (Accenture and CC)



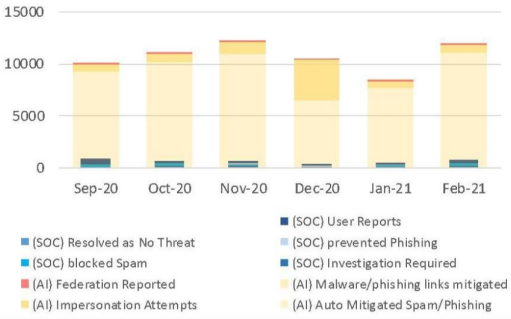
Common Digital Platform (Status 12th Feb 2021)
Qualys scan was completed on 30th Jan 2021, report has been released on 2nd Feb 2021
- All critical and high vulnerabilities have been already remediated/addressed since report released on 2nd Feb
- Outstanding Medium and Low vulnerability will target to be remediated in agreed patching/release schedule

Back Office (Status 12th Feb 2021)
Qualys scan was completed weekly basis, report has been extracted on 16th Jan 2021
- 201 out of 345 total vulnerabilities have been already remediated/addressed since report extracted on 16th Jan
- Outstanding Critical and High vulnerabilities will target to be remediated in approved patching schedule
- Risk Escalation Form has been submitted for Credence EOL RHEL servers –

Threat Intelligence



Phishing Protection (AI and SOC)



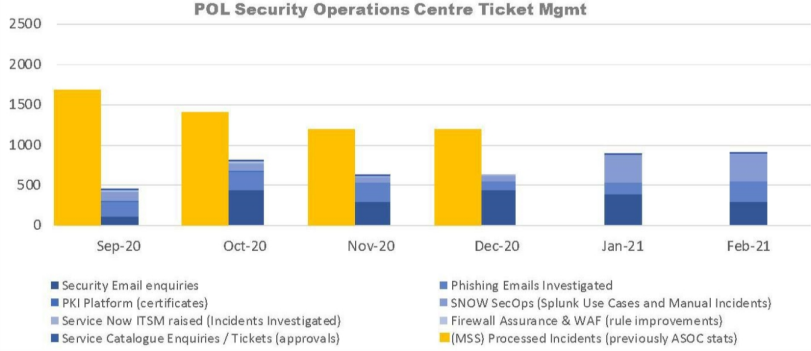
Page Break

Confidential

Post Office Limited - Risk and Compliance Committee-16/03/21

POL00423695

Cyber Operations 2



Cyber Major Incidents of note;

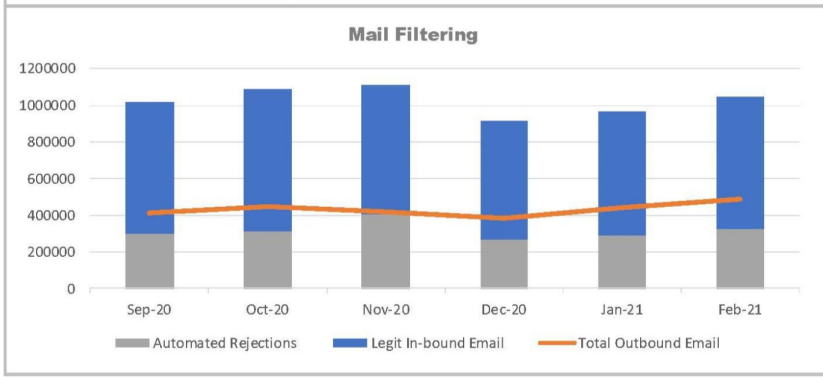
S2 - SIR0010755 - Unauthorised Access – Alert triggered for Impossible travel - user flagged with access from AWS in America, requested password & AV scan on device

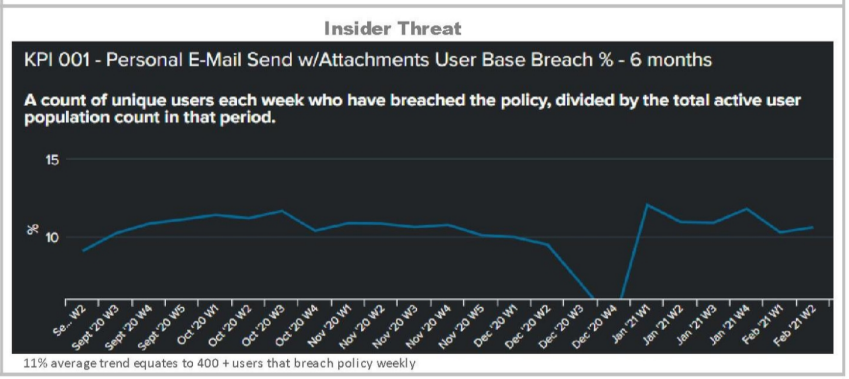
S2 - INC0342371 - Possible Counter Unit Exposed to Malware – Counter immediatly removed form service, Machine swapped out by CC engineers and shipped back to ServiceCentre for logs extraction for forensic analysis.

S3 - SIR0010748 - Possible download of emotet stage 1 – No sign of compromise requested users machine to be scanned.

S3 - SIR0010690 - Inapropiate software use; Access to TeamViewer – user flagged with brief connections to team viewer, software is not required by user and has now been removed.

S1 - SIRxxxxxxxx - Two Strictly Confidential investigations with People Management and Data Protection underway.





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

Page Break

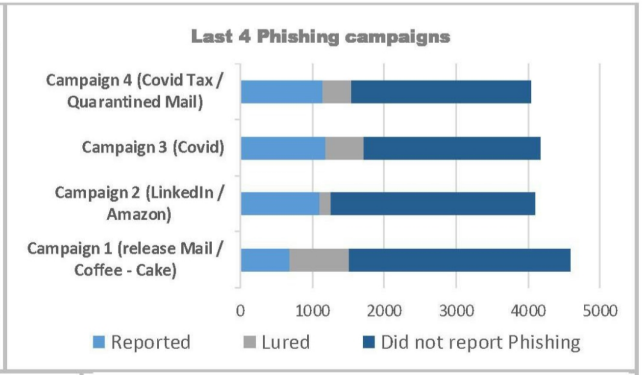
Confidential

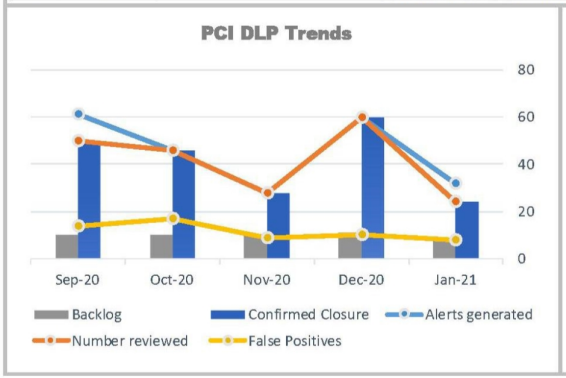
POL00423695

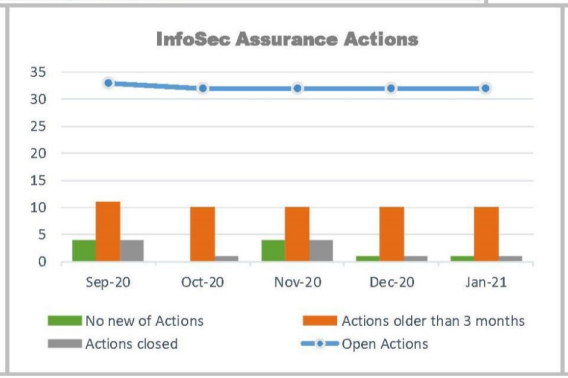
Cyber Compliance

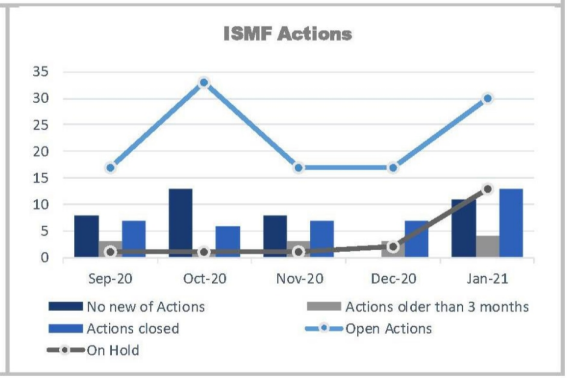
Covid-19 Tracked Major changes

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. 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. 12/11 – The migration of supporting Computacenter systems into Azure provides opportunities to review authentication and security policies as traffic routing (points of access) will be based on web gateways. Avoidance of the use of the congested VPN requires a different approach to connectivity for those colleagues not working on the POL LAN. The use of direct connectivity into O365 and Azure is being tested and will require additional authentication factors. Once this is configured, it is likely a long-term view on password expiry can be assessed.
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. 21/10 – This will be rolled into the multi-factor design being dealt with in the Computacenter response above. 12/11 – The revised connectivity model will require multifactor authentication for O365 and Azure, and connectivity to VPN is likely to become "permanently on" to facilitate patching and remote management. Device certificates and posture checking will be a feature of the VPN connectivity.
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 those are being developed. 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. 12/11 – The pilot continues and conditional access policies are being refined but the Windows 8.1 to Windows 10 migration strategy remains a dependency.
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. 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 12/11 – This is still in place (required for current lock-down) and monitoring will continue









Confidential

Post Office Limited - Risk and Compliance Committee-16/03/21

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Foreign Currency and Hedging	**Meeting Date:**	16 March 2021
Author:	Tom Lee, Financial Controller Pete Mitchell, Treasurer	**Sponsor:**	Al Cameron, Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to note:

- The process of revaluing foreign currency and the hedging of foreign exchange risk at Post Office.
- The summary of issues identified in year, the manual fix implemented and planned changes to create a better process.

6

Executive Summary

1. Post Office have a requirement to hold foreign currency inventory of notes and coins to support the travel business. They buy and sell foreign currency both centrally from First Rate Exchange Services via Hemel and at individual branch level. The Group's foreign currency risk management objective is to minimise the impact on the profit or loss account of fluctuations in the exchange rates. The Group hedges its foreign currency risk through external forward contracts.
2. The foreign exchange movements are recorded at individual currency level, by branch, in the Core Financial System on the SAP platform. Foreign currency holdings as at the end of December 2020 were manually revalued. This manual revaluation demonstrated issues with the auto-revaluation programme causing a £1.4m understatement of realised exchange differences in profit and loss account. A catchup posting was made in P9 to recognise this amount and a manual fix has been put in to mitigate this risk going forward. Post Office paid Accenture to design and implement the FX programme in SAP. A project is currently underway to fix these issues within the FX programme.

Confidential

POL00423695

Questions addressed

1. How is foreign currency revalued at Post Office?
2. Is our hedging strategy and processes fit for purpose?

Report

1. The aim of this paper is to provide an overview of foreign currency revaluation at Post Office and how the Group seeks to hedge against its exposure for foreign currency risk.

Foreign Currency

2. Post Office branches hold numerous foreign currencies that may be bought from, or sold to, customers. Reserves of foreign currency are held at the cash distribution centre in Hemel Hempstead. The bulk of foreign currency holdings relate to Euros (c.65%) and US Dollars (c.20%). Foreign currencies are supplied to Post Office by First Rate Exchange Services, the joint venture with Bank of Ireland.
3. Accounting standards require foreign currency holdings to be recorded at the spot exchange rate between the functional currency (for Post Office, this is Pounds Sterling) and the foreign currency at several points in time:
    a. Initial recognition (purchase of foreign currency).
    b. Reporting date (period end and year end).
    c. De-recognition (sale/settlement of foreign currency).

    Exchange differences arising on the revaluation of foreign currency holdings at period or year end are considered unrealised and are not immediately recognised in profit or loss. Exchange differences arising on the revaluation of foreign currency when it is sold or settled are considered realised and are immediately recognised in profit or loss. Any unrealised exchange differences relating to the sold or settled foreign currency are also now recognised in profit or loss.
4. In February 2020 an auto-revaluation programme was implemented in the Group's Core Finance System ("CFS"). Accenture built and tested the programme, with review and final sign-off performed by Post Office. The programme executes every weekend.
5. Subsequent to implementation, several interrelated issues were identified with the auto-revaluation programme, namely:
    a. The programme does not realise exchange differences in profit or loss unless the branch holding is zero when the programme is executed on a weekend.
    b. The programme assumes that exchange differences should only be realised in profit or loss if the sale results in a branch holding of zero for said foreign currency. Due to this, if the branch holding remains above zero then the exchange difference is treated as unrealised. There is no partial recognition of exchange differences in profit or loss for currency sold during the week.
    c. When the branch holding is zero at the point of revaluation, the programme realises exchange differences in profit or loss. However, there is no associated posting to clear out the unrealised exchange difference to profit or loss. Due to this, the unrealised value builds up on the balance sheet, even if the associated foreign currency has been sold.
6. Foreign currency holdings as at the end of December 2020 (P9) were manually revalued and have been revalued monthly since. This suggested that the issues with the auto-revaluation programme had caused a £1.4m understatement of realised exchange differences in profit or loss. A manual journal adjustment has been posted into CFS to correct

Confidential

POL00423695

the profit or loss account, which was effectively a catchup journal for balances which should have flowed within the year.

7. POL were reliant on Accenture's design of the FX programme and hence guided by them on the initial proposal. A common approach adopted by many organisations who do not have internal expertise
8. Accenture have been re-engaged to investigate and correct the issues identified in the auto-revaluation programme. This work is currently underway and is expected to deliver a solution by [year end]. We are working closely with Accenture to ensure that the revised programme is thoroughly tested and addresses all issues identified.
9. In addition, the foreign currency revaluation process at Post Office has been reviewed, and the following improvements are to be implemented by [year end]:
    a. Responsibilities consolidated into Treasury, facilitating more oversight and control over the end-to-end process.
    b. Bi-monthly manual revaluation performed, providing a timely sense-check against the auto-revaluation programme so that discrepancies can be quickly escalate and investigated.
    c. New validation checks and re-calculations built into the balance sheet reconciliations for foreign currency general ledger accounts, providing additional assurance over the accuracy of the auto-revaluation programme.

Hedging

10. The Group is exposed to foreign currency risk resulting from balances held to operate Bureau de Change services. The Group's foreign currency risk management objective is to minimise the impact on the profit or loss account of fluctuations in the exchange rates. The Group hedges its foreign currency risk on Euros and US Dollars, principally through external forward foreign currency contracts to cover near-term future revenues with a number of providers, including First Rate Exchange Services Holdings Limited.
11. FX hedging strategy has been reviewed and benchmarked. POL are hedging 80-120% of their exposure, up to a five weeks in the future. This in line with market practice using FX forwards to manage the exposure. Minor adjustments could be made to both the length and the percentage of hedges, this would not have negated the issue.
12. The FX hedging process is split into 2 parts, the calculation of the hedge is prepared by the Commercial team and executed by the Treasury team. Up until December 2020 when the FX issue was highlighted there was minimal review and oversight by the Treasurer. A monthly review with the commercial team is now in place. We are also discussing the options to give Treasury more control of the end to end process. All hedges are currently recorded on a spreadsheet, which is saved on a secure SharePoint site, however, this opens up risk to manual errors when recording the hedges and is not best practice. We currently place all hedges with one bank and the process is managed by Email and telephone, this is not best practice.

Conclusion

13. The hedging strategy and processes are not the reason for the FX issue, there is some room for improvement but there is no material issue or risk with the hedging.
14. The SAP FX programme implemented by Accenture in February 2020 to revalue the Balance Sheet and post realised gains and losses is not working as expected, overstating the cash position and understating the Profit and Loss, as a result of not sweeping balances to the

POL00423695

Profit and Loss. The issue was not discovered early, due to the cumulative nature of the problem and reduced trading levels, masking the issue.

15. A good implementation partner should have manually revalued the solution for us, for at least three months post Go Live, to ensure programme was working in different levels of trading. We are paying a premium to Accenture for their depth of expertise.
16. POL were reliant on Accenture's design of the FX programme and hence guided by them on the initial proposal. A common approach adopted by many organisations, who do not have internal expertise to lean on. Other Treasurers and SAP experts I consulted share my view on this. We pay Accenture because they are the experts in SAP development and solution design.

Actions

Action:	Owner	Completion Date
Realised Gains and Losses for the identified calculation errors manually recalculated	Tom Woodhouse	Monthly until fix in place
Create Request to Quote (RTQ) for Accenture containing the Target actions	Pete Mitchell/Tom Woodhouse	19/03/2021
Accenture to quote time and cost to complete the Target actions	Accenture	26/03/2021
Treasury to start 2nd review of Balance Sheet reconciliations associated with FX movement	Pete Mitchell	12/03/2021
Implement automated FX trading process	Pete Mitchell	23/04/2021

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	H2 Legal Risk Report 20/21	**Meeting Date:**	16 March 2021
Author:	Sarah Gray, Group Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting

The RCC is asked to note this report and endorse current actions designed to mitigate the risks identified and suggest any further actions that should be implemented.

Previous Governance Oversight

- Previous Annual Legal Risk Reports 2017- to date
- Post Office RCC meetings in March 2020 and September 2020; and
- ARC meetings in March 2020 and September 2020.

7

Executive Summary

1. [redacted]
2. [redacted]
3. [redacted]
4. Appendix 1 contains a high-level commentary of those risks, the current controls in place to mitigate against those risks and the further work that has been undertaken in the 2020/21 financial year and the future actions to enhance those controls.
5. [redacted]

Strictly Confidential & Legally Privileged

POL00423695

[redacted]

6. [redacted]

7

7. [redacted]

(i) [redacted]

(ii)

Questions addressed

1. What are the key legal risks?
2. What governance and assurance is in place to control those risks?
3. What is the overall position and is further action required?

Strictly Confidential & Legally Privileged

POL00423695

Appendix 1: Annual Legal Risk Report

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
	[redacted]			

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
	DVLA that Post Office was not meeting contracted			
	[redacted]			

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
[redacted]				

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
	[redacted]	[redacted]		

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
[redacted]				

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]				

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
	[redacted]	[redacted]		[redacted]
[redacted]				
	business in a timely manner impacting the business			

Strictly Confidential & Legally Privileged

POL00423695

Key Legal Risk	Performance of Risks	Control Environment	Post Control Impact Assessment	Future Actions and Responsibility
	[redacted]	[redacted]		

Strictly Confidential & Legally Privileged

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	16 March 2021
Author:	Sarah Gray, Group Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting

The Board 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

8

There are 6 matters for the Committee to note (details of which are set out in the Appendix):

1. **The Restriction of Public Sector Exit Payments Regulations 2020 revoked**
   The Restriction of Public Sector Exit Payments Regulations 2020 ("the Regulations") came into force on 4 November 2020 and set a £95,000 cap on exit payments ("the Cap") for public sector authorities. After extensive review of the application of the Cap, the Government has concluded that the Cap may have had unintended consequences and the Regulations were revoked from 12 February. HR have identified one former employee who was affected by the Cap and will be entitled to the additional sums that would have been paid had the Cap not been applied.

[redacted]

3. **Public Contract Regulations ("PCR") Post-Brexit**

   The key changes to PCR following the UK's separation from the EU are mostly practical changes which will impact how POL conducts its new procurements from 1 January 2021, including limitations on the enforceability of EU law and treaties; introduction of "Find a tender service" the new UK e-notification service to replace OJEU; and inflight procurements, new procurements and concluded frameworks. Procurements inflight as at 1 January will continue to be subject to the unamended PCR regulations. New procurements will be subject to the amended PCR regulations. Also, the operation of framework agreements concluded prior to 1 January will be subject to the unamended PCR regulations. POL is compliant with the post-Brexit requirements.

Strictly Confidential

POL00423695

4. State Aid - Update

A consultation (closing at the end of March) has been launched on the proposed approach for establishing a new subsidy control regime to replace the state aid regime of the EU. POL is preparing a response.

5. FCA finalised Guidance on the Vulnerable Customer

The FCA have issued finalised Guidance for firms on the fair treatment of vulnerable customers. The Guidance highlights the actions firms should take to understand the needs of vulnerable customers to make sure they are treated fairly. This has become a key focus for the FCA due to the impact of coronavirus. Post Office Compliance Team have been aware of the guidance and are considering the collection of vulnerability data to assist with their review of current practices.

6. Trial Witness Statements in the Business and Property Courts

From 6 April 2021, witness statements for use at trial in the Business and Property Courts only will have to comply with the newly published Practice Direction 57AC (the "PD"). [redacted] nor will it have any impact on the Public Inquiry. It was introduced following judicial disapproval of witness statements crafted by lawyers containing extensive reference to documents rather than embodying the language of the witness. It makes substantial changes to the preparation and content of witness statements. POL Legal will put a guidance document on the LCG Academy intranet page.

8

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.

Strictly Confidential

POL00423695

Appendix 1

1. Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
1. **The Restriction of Public Sector Exit Payments Regulations 2020 revoked**	As reported at RCC in November 2020, a Cap of £95,000 on exit payments in the public sector was introduced and applied to employees' exit payments from 4 November 2020. The Regulations provided that Post Office "must not" pay exit payments (such as those 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. However, the Government revoked these Regulations on 12 February this year.	A former employee has been identified who was directly affected by the Cap whilst it was in force. They will be entitled to request from Post Office as their former employer, the amount they would have received had the Cap not been in place.	As the Regulations have only been in force for a short period of time, Post Office does not have significant steps to undo/ reverse. Payment to a former employee who exited during the period the Regs were in force the sum they would have been due [£x] had the Cap not been in place. Future exits by senior employees may cost Post Office more as a result of the revocation of these Regs.	The Government still has the power to implement legislation and they have indicated they may have another attempt at bringing in similar regulations. Post Office HR will continue to monitor any developments. It is anticipated that if they do revisit exit cap regs, that they will only apply to new joiners rather than existing employees.	
2. **Supreme Court rules Uber drivers are workers**	[redacted]	[redacted]	[redacted]	[redacted]	

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-16/03/21

POL00423695

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	[redacted]				
3. Public Contract Regulations (PCR) post-Brexit	Post – Brexit, PCR 2015 remains but, the Public Procurement (Amendment etc.) (EU Exit) Regulations 2020 has been published as a UK statutory instrument to amend procurement legislation to reflect necessary changes required by the UK leaving the EU.	The key changes are: 1. The UK's new "Find a Tender" service for publishing contract notices went live on 1 January 2021, replacing the Official Journal of the European Union (only for United Kingdom). 2. EU references have all been deleted from PCR. 3. The Government have published new guidance for Below Threshold Contracts allowing for more flexibility. This will allow POL the option to reserve contract opportunities by location; and/or reserve contracts to SMEs/VCSEs only (subject to restrictions). 4. Cross-Border Interest test - no longer applies to England, Wales and Scotland contract opportunities. 5. EC Treaty Principles - no longer applies to England, Wales and Scotland contract opportunities. As a result of the NI Protocol Agreement where POL procures below threshold supplies into NI and there is cross border interest (ie from a supplier in a EU Member State) POL must advertise the contract opportunity and conduct a competition in accordance with the EC	For the time being, there is no reason to see why the current changes would not work or how they would not be anything but favourable for POL. POL may want to support local business and have the option to procure from local suppliers, subject to complying with POL internal procurement guidance. POL still has the option to contract with a supplier across the border but would have to follow the old process of advertising in the OJEU with the burden adhering to the competitive EC Treaty principle process. Gov Guidance in Procurement Policy Note 11/20: Reserving Below Threshold Procurements will allow POL to reserve procurements by location and or to SMEs/VCSEs. Certain restrictions apply (eg, ensuring value for money, management of risk, use of model contracts) and POL must also comply with its own internal procurement policy.	To ensure compliance, POL's Web 3 solution for contract management/e-procurement tool has been re-configured so that it interfaces with the Find a Tender Service. Procurement notices can therefore be published direct from Web 3 into the new e-notification hub. POL is otherwise ensuring compliance with the changes to PCR (of which there are few procedural changes) and the business may take advantage of the new freedom to reserve procurement. Separately, the Government has issued a Green Paper consultation on reforms to procurement law. The aim is to streamline tendering procedures, make them more open, flexible (to replace negotiated and competitive dialogue) and limit tendering (in crisis or extreme urgency). There are proposals for publication of annual pipelines and any contract amendments. The Government also aims to carry out a review of the court process and introduce a Tribunal System for some challenges and remedies other than damages. The consultation closes on 10 March 2021. The Procurement Director (Barabara Brannon) is currently reviewing the Green Paper and co-ordinating a proposal for the consultation. Anyone who wishes to contribute, should contact Barabara.	

Strictly Confidential

POL00423695

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		Treaty Principles and POL's internal procurement policy.		Thereafter, POL is to await publication of response to consultation and update accordingly.	
4. State Aid – Update	From 31 December 2020, the State Aid (Revocations and Amendments) (EU Exit) Regulations 2020 revokes EU State aid rules and the EU no longer has any power to investigate and take decisions on state aid measures granted by the UK. [The exception is state aid that affects trade between Northern Ireland and the EU – this would be subject to the Protocol on Ireland/Northern Ireland.]	From 1 January, until the UK establishes detailed rules for a domestic subsidy regime, it will be now operating under an interim subsidy regime. After 1 Jan 2020, when awarding subsidies, public authorities should take into account: 1. Giving a subsidy correctly (subject to international obligations)- a subsidy is currently defined as a measure which is given by a public authority; makes a financial or in-kind contribution to an enterprise; and affects international trade; 2. Whether the subsidies are prohibited; and 3. Whether the subsidy meets the terms of the principles in the UK-EU Trade and Cooperation Agreement (if over £350,000). The Government has launched a public consultation to consider and inform the further development of its new Subsidy Control regime. The Consultation closes on 31 March 2021. In its consultation the Government is asking for views on: • whether the UK should apply its own additional principles on subsidy control, as well as those set out in the UK-EU Trade and Co-operation Agreement • how best to ensure transparency across the system • the possible roles and responsibilities of the independent body that will oversee the new system	The new regime consists of a subsidy control system and consists of: • long-term replacement for the EU's prescriptive state aid regime, • more dynamic in providing support to businesses to encourage job creation and growth across the UK, • based on principles ensuring delivery of strong benefits and good value for money in a timely and effective way, • local authorities, public bodies and the devolved administrations in Edinburgh, Cardiff and Belfast will be empowered to decide if they can issue taxpayer subsidies.	POL is currently coordinating a response to the Consultation.	

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-16/03/21

POL00423695

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		• how this independent body could have some role in supporting enforcement of the principles, alongside normal judicial review standards • how the system could seek to introduce exemptions consistent with our international obligations (for example, natural disaster relief or in response to global economic emergencies).			
5. FCA finalised guidelines on the Vulnerable Customer	Following consultations in July 2019 and 2020, the FCA published a draft consultation Guidance for Firms on the Fair Treatment of Vulnerable Customers. The Guidance is on how regulated firms would meet the FCA Principles for Business and they apply to POMS, Capital One, BOI and POL (as an appointed representative of POMS). Since then, the business have been considering further work, notably around culture and understanding the makeup of our customer base. The FCA considers 47% of the population could be regarded as potentially vulnerable.	The FCA has now finalised its Guidance for firms on the fair treatment of vulnerable customers. The Guidance aims to provide a framework that allows firms to accurately assess whether they are treating vulnerable consumers fairly, ensuring consistency across the financial services sector. The Guidance sets out the FCA's expectations on: understanding the needs of vulnerable consumers; ensuring that frontline staff have the necessary skills and capability to recognise vulnerability; and for firms to consider the characteristics of vulnerability present in their target market or customer base and how they can meet customers' needs through the design of products and services, their customer services and their communications.	The FCA's view of vulnerability is as a spectrum of risk. All customers are at risk of becoming vulnerable, but this risk is increased by having characteristics of vulnerability. These could be poor health, such as cognitive impairment, life events such as new caring responsibilities, low resilience to cope with financial or emotional shocks and low capability, such as poor literacy or numeracy skills. As such, one key requirement for POL is to better understand our customer database. Post Office would be required to consider anything that would have an impact on vulnerability. Consideration needs to be made across the whole life cycle of a product from its design to distribution and thereafter. POL has provided vulnerable customer training on SuccessFactors and produced accessibility guidance.	It should be noted that this is guidance rather than mandatory and there is no immediate requirement to implement any changes. Notwithstanding the above, our two principals are both doing a gap analysis to review processes to evaluate where the needs of vulnerable consumers have not been met, so that improvements can be made. For example in POMS call centres they will be asking customers to self-identify their vulnerability.	
6. Trial Witness Statements in the Business	Post Office is a public body subject to scrutiny, and particularly so at the moment. On occasion, Post Office colleagues have to produce witness statements to assist with matters going before the Courts.	Applicability of the PD • Applies to witness statements for use at trials in the Business and Property Courts signed on or after 6 April 2021. • It does not matter when the claim was issued.	Post Office staff should keep in mind that if they are ever required to give a witness statement to assist in a trial, there is now more emphasis placed on witnesses' own recollection and human memory in order to avoid over-reliance on documents. In summary: do not argue, stick to the point,	POL Legal to produce a guidance note. The RAG is green on this issue as it is not considered to be a material legal development affecting the business. The changes to witness statements which the new Practice Direction	

Strictly Confidential

POL00423695

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
and Property Courts		• It does not apply to affidavits, or to other types of witness statements. The content of witness statements • Should set out only matters of fact of which the witness has personal knowledge and are relevant to the case • Should list the documents referred to • But not quote at length from any document referenced • Should not seek to argue the case or contain a commentary on other evidence in the case • must now be produced in accordance with the Court's Statement of Best Practice. Sanctions for non-compliance If a party fails to comply, the Court can • Refuse permission to rely on some/ all of the evidence • Order the witness statement to be redrafted • Make an adverse costs order • Order a witness to give some/ all of their evidence-in-chief orally.	refer to documents only where necessary, explain your recollection and ensure that certificates of compliance are given. [redacted] As regards the public Inquiry, as this is a matter for public record and does not constitute formal proceedings brought before the Business & Property Courts', again to the extent any witness testimony is to be given ahead of the Inquiry commencing, this will be unaffected by Practice Direction 57AC. Given, however, the purpose of the Practice Direction is to mitigate the judicial concern around witness statements being crafted by lawyers containing extensive reference to documents rather than embodying the language of the witness, it may be the case (from a horizon-scanning perspective) that we see similar changes made to the delivery of witness evidence more widely in other courts in the future.	necessitates are limited to statements issued in proceedings before the Business & Property Courts. Both the [redacted] and impending public inquiry fall outside the scope of the Practice Direction. Therefore, at this stage, it is just a legal development to note so in the event that, in the future, a POL employee is required to give evidence in a matter before the Business & Property Courts, they are aware of the latest obligations in producing witness evidence.	

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Business Continuity Gap Analysis	**Meeting Date:**	16 March 2021
Author:	Jonny Lonsdale (Business Continuity Manager)	**Sponsor:**	Alisdair Cameron, Chief Finance Officer

Input Sought: Noting

The Committee is asked to **note** the summary findings of the Business Continuity Gap Analysis review for Post Office Group for onward submission to the Audit, Risk & Compliance Committee (ARC).

Executive Summary

Background: In an effort to determine the status of the Business Continuity Management System ("BCMS") the Business Continuity Manager has completed a gap analysis on its alignment to the BSI ISO 22301 (Business Continuity) standard. The folders of documentation provided by Tim Armit have been assessed as part of this review.

Standard: A BCMS aligned with ISO 22301 is based on Business Impact analysis and takes into consideration the organisation as an entirety. It includes disaster recovery and business continuity plans that focus on the recovery of specific activities, operations, functions, sites, services,etc.

Conclusion: The Gap Analysis has found that the overall status of the Post Office BCMS is non-compliant with some aspects of the industry standard, and in particular the most concerning gaps are in the following areas;

1. Business Impact Analysis
2. Business Continuity Plans
3. Governance Framework
4. Exercising and Testing

Confidential

POL00423695

Questions addressed

1. Does PO have a fit for purpose BCMS in line with the BSI ISO22301 standard?

2. What changes are needed to the BCMS to meet the requirements of the standard?

Report

Audit, risk and control

4. Post Office does not have a detailed Business Impact Analysis for each department; therefore, the organisation does not have a process of determining the criticality of business activities and associated resource requirements to ensure operational resilience and continuity of operations during and after a business disruption. Although the Post Office does not have documented BIA's, the RCC and ARC should take assurance that disruption to key activities have been limited during the pandemic and its work from home strategy which displays that the organisation is aware of its key activities.

5. Not recognising the critical activities in an organisation prevents identification of risks which need to be prioritised in preparedness for a major incident resulting in an unacceptable standard of resilience. However, the Post Office manages major incidents effectively through its escalation process and should have some comfort in the response to the pandemic outbreak which limited impacts to the continuity of its products and services.

6. A departmental business continuity plan allows those accountable to design their own recovery strategy. This includes the minimum business continuity objective (staff resource), the time of which to resume the key activities and location. Although I have seen some departmental plans (Supply Chain) which detail response procedures and alternative locations, this is not replicated through the business and if we do not have these documented procedures our ability to respond to incidents will be impacted.

Stakeholder and workforce engagement

7. A group of Business Continuity Plan owners and BIA Champions have been identified to roll out the refreshed BCMS. These stakeholders will be required to complete a Business Impact Analysis and Business Continuity Plan with the guidance of the Business Continuity Manager. Completion of these sessions will be held on a 1-1 meeting basis to ensure the information is completed effectively and consistently.

Critical Systems

8. It is also noted that the critical branch supporting system, Horizon, has not been fully disaster recovery tested therefore confidence in that the system would remain operational in the event of a Data Centre outage is not established. Testing on Horizon is planned for this year and it is expected a full failover test will be completed.

Financial Impact

3. There is limited financial impact to implement the refreshed BCMS. However, a Service Now module has been identified as a useful tool to aid the BCMS effectiveness although

Confidential

POL00423695

this is in the early stages of discovery therefore no business case has been put forward for approval.

Risk Assessment, Mitigations & Legal Implications

4. The present work area recovery strategy for the Chesterfield office is to relocate to the SunGard site in Leicester. This contract expires on the 31st March and a decision has been made not to extend the contract. The Post Office is aware of the risks associated with ending this contract and have plans in place to mitigate this. With many colleagues now working from home this decision will have limited impact. If laptops are damaged in an incident, there may not be enough spare laptops in storage to replace a large number. A desktop strategy is currently being considered with IT in order to mitigate this risk and for colleagues to leave laptops at home when coming to work in one of the offices.

5. There is no defined list of up to date critical suppliers of products and services that support the strategies of the BCMS. This may result in not identifying risks associated with suppliers which could be mitigated or used to plan contingencies if they become unavailable. For example, COVID response, impacts and business resilience.

6. A list of our most high value or most dependent external partners have not been established which prevents appropriate Business Continuity strategies being developed to ensure we meet the needs of those customers. By creating this list, we can identify our SLAs and ensure these timescales can be achieved in the event of a Business Continuity incident.

Stakeholder Implications

7. Each department or team will be required to complete a BIA during Q1 with the assistance of the Business Continuity Manager. Each BIA will take approximately 1 hour to complete with an additional hour for the Business Continuity plan.

8. There is a risk that due to the lack of training and awareness for colleagues in regard to the identification of Business Continuity risks we currently a number of unknown risks which require mitigation in order to ensure the Post Office can continuity to provide its products and services at an agreed level. A competency matrix will be established to identify what training would be the most appropriate for the BCMS stakeholders.

9. Once BIA's and Business Continuity plans have been created, a series of scenario-based testing exercises will be scheduled that each Business Continuity plan holder will require to attend. The Gap Analysis found that one department of the organisation has a robust testing and training programme of Business Continuity activity in place which was Supply Chain.

10. An annual audit should be agreed for our Internal Audit team to review the BCMS against the BSI 22301 standards to ensure a degree of compliance is achieved and improvements measured following this gap analysis.

Confidential

POL00423695

Other Options Considered

11. Implementing a BCMS framework is to inform and drive continual, effective, cross-functional, multi-level continuity planning through holistic, integrated risk management practice in the following ways;

12. Establish a control environment to link corporate governance, risk management, business planning and operational performance to the Post Office strategic direction (business continuity programme);

13. Invest time, tools and techniques to ensure BCMS is a fully embedded, auditable business management process;

14. Provide senior managers with opportunities to obtain a sound understanding of business continuity management and requisite skills to implement business continuity effectively;

15. Ensure the framework is sufficiently flexible to meet the challenges of scalability, different department business profiles and various geographic needs coupled with governance, regulatory and legal regimes;

16. Assist and manage events that require information and resource coordination across multiple business functions;

17. Uphold a resilience philosophy in which the Post Office business continuity capability always reflects the needs, technology, structure and culture of its business.

Next Steps & Timelines

18. For Post Office BCMS to achieve compliance with ISO22301 standard the following BCMS schedule of work is to be completed over the course of the next 12 months;

Q1	Q2	Q3	Q4
Creation of BIA	Create BC Plans	Testing Schedule	Plan Internal Audit of BCMS
BIA Roll Out	Create Internal / External Incident Communications statements	Create Competency Matrix for Stakeholders	Create BCMS annual workflow
Identify Key Suppliers & Review BCP Status	Create BC Sharepoint site for document repository	Create Improvement Tracker	
Identify Contractual Obligation	Training & Awareness Sessions		
Create Framework Document	Create BCMS invocation Severity Matrix		

Confidential

POL00423695

Review and update BC Risks in Risk Register (SNOW)	Review Business Continuity Policy		

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Payzone Bill Payments Deep Dive Report	**Meeting Date:**	16 March 2021
Author:	Michelle Embrey, Quality & Risk Manager	**Sponsor:**	Andrew Goddard, Payzone Bill Payments Managing Director

Input Sought: Noting

The Committee is asked to note the Payzone Risk & Compliance Update report for onwards submission to the Audit, Risk & Compliance Committee (ARC).

Previous Governance Oversight

This is a follow up action for a deep dive from the previous ARC meeting on 22nd Sept, 2020.

Executive Summary

This paper provides a summary of the following items within the Payzone Bill Payments (PZBP) business:

- Key risks and mitigations
- Internal governance
- Compliance with regulation
- Internal audit
- Complaints and whistleblowing
- Customer and employee satisfaction

A comprehensive risk register exists within PZBP, with mitigations in place and reviewed monthly by the senior management team. Improvements in the internal governance have been implemented in the areas of risk management, change control, business continuity and information security as well as the ongoing project to align key PZBP policies with the Post Office (POL). The internal audit conducted by POL concluded that the control environment in PZBP is appropriate for the size and complexity of the organisation. Ownership of the PZBP legal register has been transferred from POL group legal to PZBP and reviewed annually at the PZBP Board.

10

Complaint handling improvements have been identified to incorporate feedback from customers, retailers and client. The overall Trustpilot scores remain high at 4.5, reflective of strong retailer and customer helpdesk support, with some of the highest scores in the last 12 months in Period 11. Employee satisfaction levels remain positive, with small negative changes in wellbeing during the lockdown, and engagement following the first of two major organisational restructures within 6 months.

Overall, the business has progressed significantly in incorporating controls, policies, and risk management practices, with further improvements identified and resourced.

Questions addressed

1. What are the key risks within PZBP and what are the mitigations for these?
2. How is the internal governance embedded into the PZBP operation?
3. Are PZBP fully compliant with relevant regulations?
4. What is the complaints and whistleblowing process?

Confidential

POL00423695

5. What are the customer and employee satisfaction levels?

Report

1. Key Risk

The following risks are extracted from the PZBP risk register that is aligned with the POL risk register;

a. Intermediate Risk – the ability for PZBP to deliver the 5 yr plan (risk score 9)

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.

b. Poor trading conditions in the current pandemic (risk score 9)

The lockdowns during 2020/21 have had a significant impact on the bill payment trading conditions with performance running behind original budget whilst holding up against LY at 95%, and 96% of target (year to date week 49). Performance has been impacted due to vulnerable customers shielding at home, clients working with customers to offer credit and payment holidays, and branch and store closures/reduced opening hours driving non-cash customers to pay through alternative means. We have continued to negotiate with key clients by signing new Energy clients in Bright and Jersey and driven new volume from agreements re-signed with E.On, EDF and via our energy platform partners, Siemens and Itron, and we will drive additional revenue from new deals with Allpay and Capita.

c. The impact of the Covid-19 pandemic on clients (risk score 6)

We are starting to see some of the smaller Energy companies struggle and fail due to bad debt and cash flow impact. Their customers however are being absorbed by the big 6 suppliers e.g., Robin Hood Energy taken over by British Gas, and this will drive transactions into our networks. The transport industry has been significantly impacted and will continue until people can travel freely, albeit we have positive engagement with the likes of National Express Coach & Bus, GoAhead, First Group, Transport for Wales, and Lothian Bus.

d. The long-term impact of the pandemic on finances (risk score 6)

Notwithstanding the changeable impact from Covid-19, the actions completed within the PZ credit management function has resulted in a reduction in retailer debt to below the levels seen pre-pandemic at only 0.5% for failed direct debits and a collection rate at 99%. Close daily monitoring and integrated credit, helpdesk and field support have resulted in the improved performance.

e. The dependency on third parties (risk score 6)

Confidential

POL00423695

Throughout the 12 months of the 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 PZBP's device 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.

2. Internal Governance

a. Responsibilities

The PZBP Board of Directors are responsible for the overall business strategy and ensuring that an efficient system of internal controls are in place. These functions include risk management, compliance, internal audit, change control, financial accounting, information security and business continuity.

The senior management team are responsible for overseeing the process of communications with the board by regularly reporting and informing on relevant aspects and be actively engaged with the business to enable well informed decisions. The senior management team also oversees the implementation of the strategy, the risk culture, code of conduct and the integrity of the financial information. The senior management team identify, manage and mitigate actual or potential conflicts of interest.

b. Framework

PZBP have ensured that the organisational framework is suitable, effective and transparent. The effectiveness is a result of appropriate human resource allocation.

A particular focus being on the improvement of the following internal controls:

- Improvement of the risk culture and management
- Change control with the implementation of the change advisory board and will be further enhanced with the introduction of the gating process
- Business continuity and information security evidenced by PZBP's ability to efficiently continue operations in the current pandemic crisis and the achievement of the UKAS accredited certifications ISO 27001 information security and ISO 22301 Business continuity.

The overall framework and relationship with POL governance is detailed in the process flow map in Appendix 1.

c. Policy Update

In an effort to align the key policies within PZBP, a gap analysis exercise was conducted comparing PZBP and Post Office policies. The result of this was a list of 28 policies that should be adopted, or PZBP specific policies created where adoption is not possible.

This paper provides a summary of the current status of the review with full detail in Appendix 2. The recommendations put forward to the PZBP board are as follows:

- Adoption of 19 policies with no addendums or variations which will be submitted to the PZBP April Board meeting

Confidential

POL00423695

- A variation required for 1 policy (the variants of Modern Slavery and Vulnerable Customer have already been approved by PZBP board), to be actioned by the July PZBP board meeting
- There are 5 policies that are currently classed as under review and will be implemented by the July PZBP board meeting

3. Compliance with Regulation

Compliance with regulations within PZBP is externally audited by a UKAS accredited certification body as part of the ISO 27001 Information Security and ISO 45001 Occupational Health and Safety certifications. PZBP were found to be compliant with applicable legislation.

A dedicated PZBP legal register is now managed by PZBP Legal Counsel and linked into the POL legal register and is reviewed annually by the PZBP Board.

4. Internal Audit

An internal audit was conducted within the finance and IT functions by the POL audit team in 2019. This audit concluded that the control environment in PZBP is appropriate for the size and complexity of the organisation. There were 15 findings raised and of these only 2 are ongoing (See Appendix 3), to be completed by August 2021. PZBP are due to be audited again in Q1 of the 2021/2022 auditing schedule once the schedule is approved by ARC.

PZBP have 2 internal auditors responsible for the internal audit programme across all functions within PZBP. This process assesses the quality of the internal control framework by reviewing existing policies and procedures to ensure they remain suitable and comply with the requirements of the ISO certifications. PZBP is also externally audited as part of the UKAS accredited ISO standards. PZBP are currently certified to the following ISO standards:

- ISO 9001:2015 Quality Management Systems
- ISO 45001:2018 Occupational Health and Safety Management Systems
- ISO 14001:2015 Environmental Management Systems
- ISO 27001:2013 Information Security Management Systems
- ISO 22301:2014 Business Continuity Management Systems

5. Complaints and Whistleblowing

The total number of customer complaints logged during 2020 were low, with an average of just 2 complaints per month.

There are a series of improvements to the made that have been instigated and will be completed by Q3 2021

- SLAs to be introduced on response and completion
- Targets should be introduced and linked into business KPI's
- Complaints to be formally defined to ensure all complaints received are logged
- Technical upgrade to CRM system to capture complaints
- Complaint reporting to be included in business performance KPI's regularly communicated to the senior management team.

POL00423695

There have been no instances of whistleblowing within PZBP during 2020. However, a number of improvements have been identified, including adopting the group Whistleblowing policy, appointing a whistleblowing officer and improved awareness of the process. This will be completed by the July PZBP Board meeting

6. Customer and Employee Satisfaction

a. Customer Satisfaction

The customer satisfaction is currently evaluated via a monthly customer satisfaction survey and ongoing Trustpilot reviews. The results from the 2020 data show that customer satisfaction is high with a Trustpilot score of 4.5 and the customer satisfaction survey producing an average satisfaction level of 94%. Appendix 5 highlights the improving Trustpilot scores with P11 showing the highest scores in the year against categories such as friendly, going the extra mile, and overall satisfaction. Any retailers that are highlighted via these channels that have provided a customer with a poor service are issued an etiquette form and followed up, and this process needs to be enhanced.

There are a series of improvements that are currently being implemented and are scheduled for completion August 2021

- Alignment of the PZBP surveys to the POL survey
- Customer satisfaction follow-up process and reporting
- NPS improvements

b. Employee Satisfaction

PZBP has assessed employee satisfaction via two pulse surveys in both April and December 2020. The individual pulse surveys showed an increase in mental and physical wellness from April to December and also showed a slight increase in individuals' productivity in this same period. This increase from April to December is likely to be a reflection of employees accepting the working from home requirement that was introduced in March 2020, in response to the pandemic crisis. There was also a major restructure implemented in September 2020 which explain the few areas that saw a minor decrease in satisfaction (see Appendix 4). The high-level responses collated from these pulse surveys were presented to the management team. Engagement champions were involved in order to generate and implement the action plan.

A further pulse survey will be released in April 2021 and full engagement survey will be released in November 2021, and then annually thereafter.

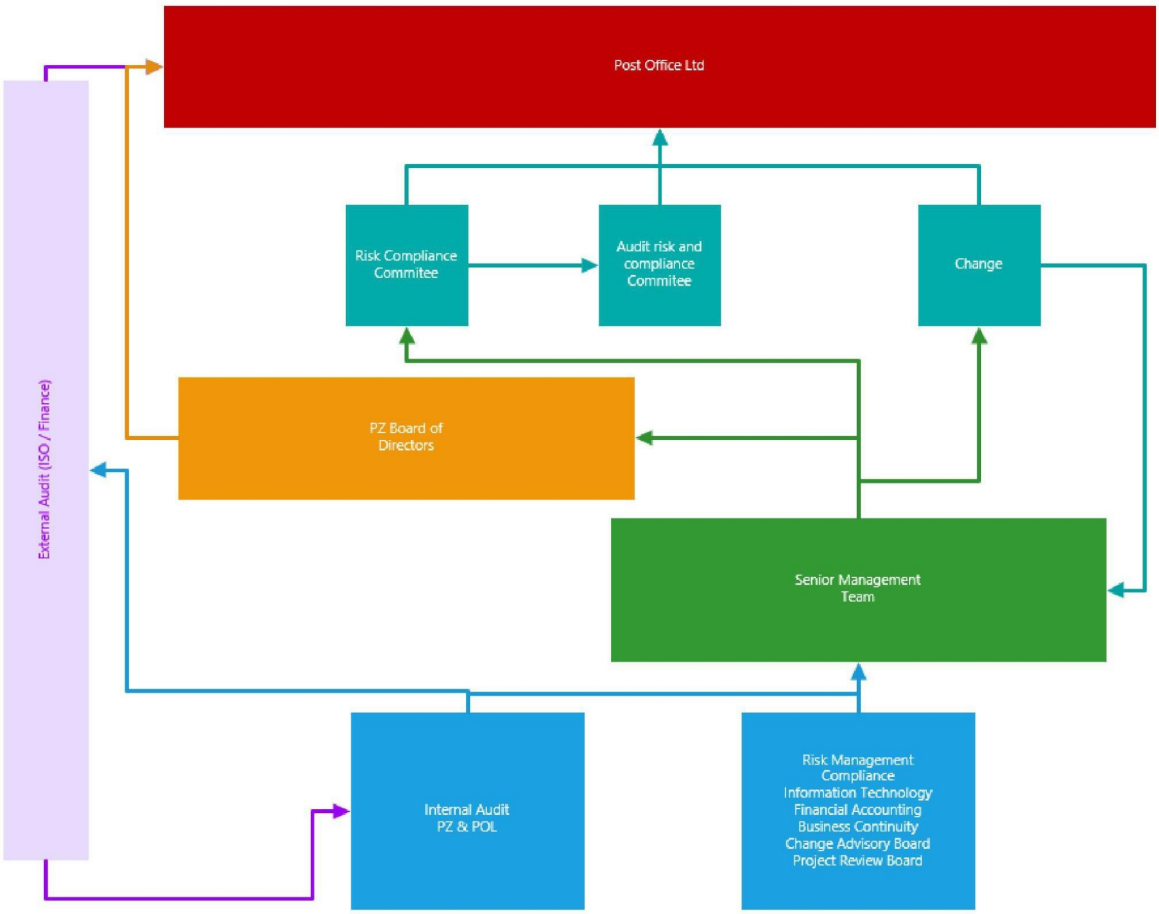
Next Steps & Timelines

7. The key group policies recommended for adoption to be submitted for approval to the April 2021 PZBP Board meeting, with the physical security variation and review of the remaining key group policies submitted to the July 2021 PZBP Board meeting.
8. The implementation of the complaints process improvements scheduled to commence May 2021, customer satisfaction improvements to be implemented by August 2021, pulse survey in April 2021 and the engagement survey will be released in November 2021.

Confidential

POL00423695

Appendix 1: Governance Framework



10

Confidential

POL00423695

Appendix 2: Policy Update

Department	Policy	Recommendation			Justification
		Adoption	Variation	Review require	
Corporate Governance	Conflict of Interest	✓			
	Contract execution	✓	✓		
	Modern slavery statement		✓		Current statement can not be adopted due to PZ not having DMBs. PZBP could be included in future iterations with amendments
Risk	Risk Appetite Statement	✓			
	Risk	✓			
Financial Crime	Financial crime	✓			
	Anti-money laundering & counter terrorism funding	✓			
	Vulnerable customer		✓		Current policy can not be adopted due to PZ not having DMBs
	HMRC fit & proper standards			✓	
	Anti-bribery & corruption	✓			
Business Continuity	Business continuity management	✓			
Legal	Investigations			✓	Investigations policy is in draft form
	Law enforcement agencies	✓			
Data Protection	Freedom of information	✓			
	Protecting personal data	✓			
	Document retention policy	✓			
Internal Audit	Internal audit charter	✓			
IT	IT DR	✓			
Cyber Security	Cyber & information security	✓			
Procurement	Procurement			✓	Procurement policy is in draft form
Health & Safety	Health & safety			✓	Discussion with MH with regard to applicability to PZBP
Physical Security	Physical security		✓		
Human Resources	Conduct Code	✓			
	Code of business standards	✓			
	Whistleblowing		✓		An adendum will be required to include PZ specific whistle blowing manager and contact details
	Equality diversity & inclusion	✓			
Finance	Post Office treasury			✓	Further review by an individual with specific experience

10

Confidential

POL00423695

Appendix 3: Internal Audit

	Finding	Rating*	Action Owner	Date	Response	Status
Finance						
Scope Area: Governance						
1.	Financial policies and processes do not fully reflect the current operation	P2	Stephenie Smith	31/12/19	The main process are documented. Further work required regarding VAT and debtman but these are due to changes. Completion date scheduled for July 2021	Ongoing
2.	No formal internal delegation of authorities matrix	P2	Stephenie Smith	30/11/19	Document of authority has been created and authorised. Last reviewed Dec 2020	Complete
Scope Area: Core Financial Processes						
3.	Goods Receipting is inconsistent	P3	Stephenie Smith	31/12/20	This is mitigated by ensuring that the invoice is approved by the originator prior to payment being made	Mitigated
4.	Client Trust bank accounts remain in the name of PZUK	P2	Stephenie Smith	25/10/20	A TSA is in place with Takepayments. A project is underway to enable the separation of the banking structure. Completion date scheduled for Aug 2021	Ongoing
5.	Credit Control policy does not reflect actual merchants credit limits or payment terms in operation	P2	Andy Munro	31/12/19	Credit limits have been set and the policy updated to reflect this	Complete
Scope Area: Retail						
6.	Process for the onboarding of new merchants is not documented	P3	Andy Munro	31/12/19	The onboarding process has been documented within the updated Credit Control policy	Complete
IT						
Scope Area: IT Governance						
7.	IT Strategy is not fully defined or documented	P2	Lee Blackburn	31/3/20	The PZ IT strategy is now clearly defined. The overall objective of the strategy is to reposition its core system hosting platform into AWS whilst delivering IT software solutions centred on product offerings (Energy, telco etc). Supporting these offerings are a consistent device strategy that underpins the offerings of the PZ business and also additional post office services where applicable.	Complete
Scope Area: System Development						
8.	Coding standards are not defined	P2	Ralph Wort	31/3/20	PZ it uses a consistent development framework that is underpinned by the over-arching strategy. In addition to industry frameworks we also adopt internal policies and procedures such as peer reviews, internal audits etc. Structured coding standards are at the	Complete

POL00423695

					core of our software development processes	
Scope Area: Infrastructure and Systems Integration						
9.	There are no processes for ongoing third party assurance	P2	Neil Davey	31/3/20	Supplier code of conduct and questionnaire in place	Complete
Scope Area: Access Controls						
10.	There are no JML processes for dormant AD or application accounts	P2	Michelle Embrey	31/12/19	The JML process has been documented	Complete
11.	No monitoring of wireless network creation	P2	Lee Blackburn	31/12/19	Only admin users (IT Ops) can create SSIDs. JD has disabled discoverable feature on all machines	Complete
12.	The Sophos XG firewall controlling traffic into and out of the Northwich HO location is not securely configured	P2	Lee Blackburn	31/12/19	Fire wall is for internet monitoring and control only (block FTP). Mitigation in place: Filters in place to stop malicious content, end point protection (Sophos), User names and passwords required for logins, IT Ops admin accounts, Firewall in DC controlled and managed by Vodafone@ IP address level. POL auditor wanted network level firewall, implementing this will cause disruption and incur extra cost. This is an unnecessary action	Complete
13.	Lack of consistency of controls over physical access to Northwich site	P3	Michelle Embrey	30/11/19	Reminder email has been issued detailing the importance of keeping the reception door closed. Visitors and contractors must sign in.	Complete
Scope Area: IT Security and Operations						
14.	Patch management processes are not fully documented	P3	Lee Blackburn	31/12/19	The patch management process has been documented within the Patch Management Policy	Complete
Scope Area: Data Privacy						
15.	Data Protection processes not yet integrated	P1	Michelle Embrey	31/12/19	The data breach and information request processes have been implemented and training is currently being rolled out to the organisation.	Complete

Confidential

POL00423695

Appendix 4: High-level Pulse Survey Results

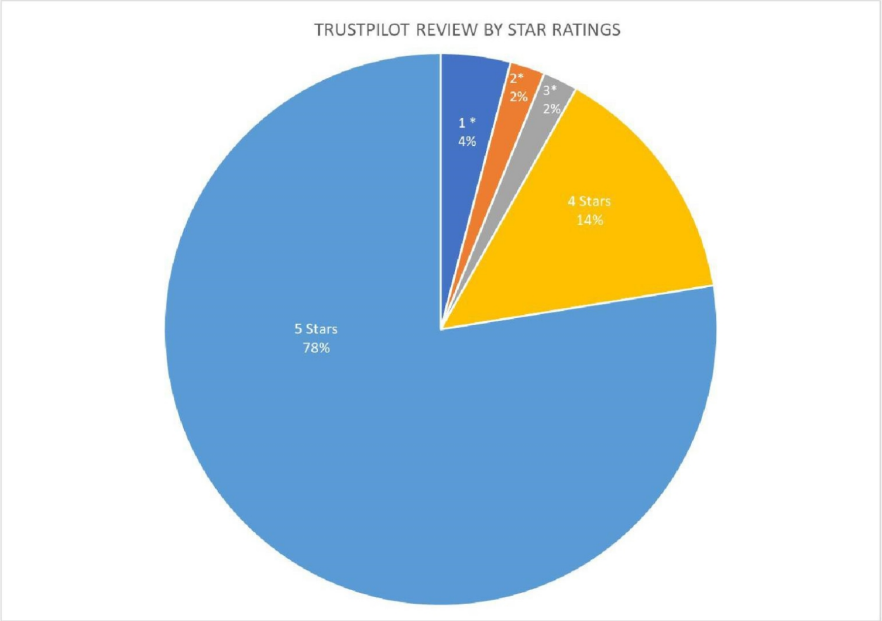
December 2020 Pulse Survey	April 2020 Pulse Survey
53% response rate	75% response rate
100% of respondents are feeling between great and okay physically	93% of respondents were feeling between great and okay physically
98% of respondents are feeling between great and okay mentally	94% of respondents were feeling between great and okay mentally
93% of respondents say their current working environment enables them to be productive within their role	91% of respondents said that their current working environment enabled them to be productive within their role
83% of respondents say that their work schedule is flexible enough for them to balance their responsibilities between family & personal.	91% of respondents said that their work schedule was flexible enough for them to balance their responsibilities between family & personal
93% of respondents say that their manager listens to their ideas and feedback	95% of respondents said that their manager listen to their ideas and feedback
84% of respondents say that their line manager creates an environment which encourages team collaboration and clarify of direction	91% of respondents said that their line manager creates an environment which encourages team collaboration and clarify of direction

Confidential

POL00423695

Appendix 5: End user Customer Satisfaction Results

		Driver Score	Friendly	Professional	Knowledge	Understanding	Efficiency	Expectations	Ease	Clean & Tidy
Year 2020/21	Period 01	92.20%	91.50%	92.10%	91.70%	92.90%	91.90%	93.20%	89.50%	90.80%
	Period 02	95.80%	95.80%	96.30%	95.40%	95.60%	95.80%	96.00%	92.90%	94.00%
	Period 03	93.60%	94.20%	93.50%	93.90%	93.90%	93.20%	93.00%	92.10%	89.90%
	Period 04	95.20%	95.60%	95.00%	94.70%	95.20%	95.40%	95.20%	94.30%	91.90%
	Period 05	94.50%	95.30%	94.50%	94.10%	93.40%	95.00%	94.50%	93.40%	94.60%
	Period 06	95.60%	95.30%	96.00%	95.00%	95.50%	96.20%	95.80%	93.20%	91.80%
	Period 07	96.10%	96.30%	96.30%	96.00%	96.00%	96.00%	96.00%	94.10%	93.80%
	Period 08	93.50%	94.30%	93.80%	92.70%	93.80%	93.10%	93.60%	93.10%	92.00%
	Period 09	94.40%	93.90%	95.00%	93.70%	94.80%	94.10%	95.00%	92.20%	91.60%
	Period 10	93.10%	93.50%	93.70%	92.50%	92.30%	93.10%	93.50%	91.50%	89.90%
	Period 11	96.70%	97.10%	97.00%	96.80%	96.90%	96.30%	96.20%	93.70%	92.80%
		Wait Time Acceptable	**Satisfaction**	**Emotional Impact**	**Perceived Wait Time**	**Clear Directions**	**Average (PERCEIVED WAIT TIME)**	**Extra Mile**	**Opportunity**	**Response**
	Period 01	96.00%	90.80%	77.50%	74.10%	92.70%	3.65	372	13	524
	Period 02	97.40%	95.30%	85.80%	74.10%	94.70%	3.73	740	10	910
	Period 03	95.90%	93.30%	83.30%	77.50%	92.60%	3.23	399	5	556
	Period 04	97.80%	94.30%	83.00%	82.30%	93.80%	2.77	413	10	546
	Period 05	96.70%	92.90%	85.60%	86.80%	94.80%	2.54	297	4	424
	Period 06	96.50%	93.90%	85.90%	86.80%	94.10%	2.55	321	5	425
	Period 07	97.90%	95.40%	88.40%	88.50%	95.80%	2.38	1,258	28	1,553
	Period 08	95.80%	92.40%	85.10%	82.20%	92.90%	2.84	411	11	550
	Period 09	96.30%	92.90%	87.10%	71.60%	93.30%	3.52	336	8	464
	Period 10	95.60%	91.90%	85.00%	79.70%	92.10%	3.15	512	11	680
	Period 11	98.40%	96.00%	89.20%	84.20%	95.90%	2.73	1,047	10	1,285



10

11

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Prohibited and Restricted Items Progress Update	**Meeting Date:**	16 March 2021
Author:	Mike Elliott, Network Sales Development Manager	**Sponsor:**	Andy Kingham, Franchise Partnering Director

Input Sought: Noting

The Committee is asked to note:

i. the activity undertaken and planned in order to improve conformance to the required process; and
ii. the anticipated improvement in mystery shopping conformance as a result of the proposed system changes.

Executive Summary

Since 2012, Post Office has contracted with Royal Mail to help meet its obligations to the CAA (Civil Aviation Authority) for checking the list of prohibited and restricted items and any applicable packaging, volume, quantity, labelling and product restrictions that apply prior to posting any item. Royal Mail provides a comprehensive A-Z list that gives detailed information about the things that cannot be posted with us, or where restrictions are in place and covers all our UK mail and International mail services. This list of prohibited and restricted items reflects Royal Mail's general terms and conditions.

During the most recent audits, the CAA have highlighted that Post Office Ltd. can only act in the capacity as the first line of defence regarding the acceptance or refusal of prohibited and restricted items. Whilst the ultimate responsibility lies with Royal Mail, Post Office Ltd. takes this responsibility seriously.

11

To monitor compliance levels for Prohibited and Restricted Items (P&RI), Mystery shopping is completed on a monthly basis by IPSOS. Since its inception, POL results have been inconsistent, falling below acceptable levels in most months. Over the last 6 months compliance levels for International performance peaked at 77% and inland 56% - (latest wave was Period 9, due to mystery shopping being paused due to the pandemic).

This paper provides an update on the progress to date to deliver performance improvements and outlines the next steps we are and need to take to improve compliance levels further for the acceptance of Dangerous goods items.

Confidential

POL00423695

Questions addressed

1. Why do we need to improve conformance levels for Prohibited and Restricted items?
2. What is the impact of not doing this?
3. What steps have been implemented since the last update (July 2020) to address this?
4. What additional steps are planned to improve compliance further?
5. What is the current focus in the network to address this?

Report

1. Why do we need to improve conformance levels for Prohibited and Restricted items?

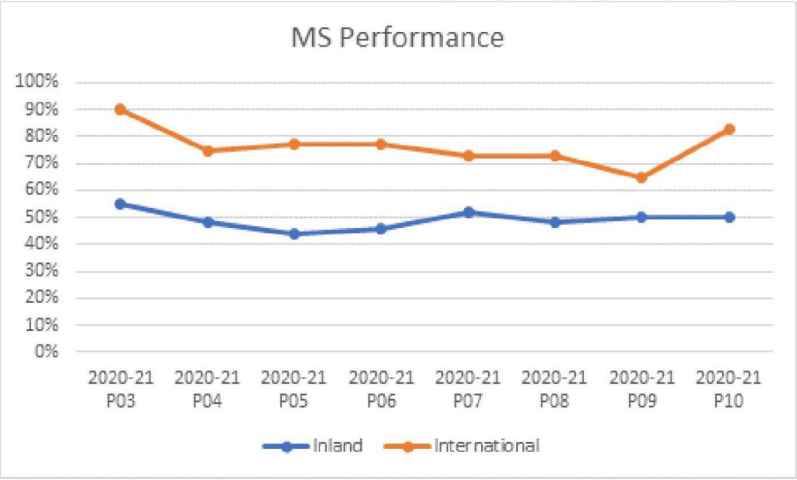
To comply with national and international regulations governing the carriage of mail, and to ensure that mail in transport does not present a danger to the general public, we restrict or prohibit certain items from entering our network and the Royal Mail pipeline.

We want to ensure the mail is safe for everyone, with many items, such as batteries, aerosols, nail varnish and perfumes (amongst other items and substances), considered as dangerous goods under transport legislation. For items posting overseas, other postal administrations may have different prohibitions and restrictions. All the individual and country specific restrictions and prohibitions add further complexity to the transaction at the counter.

Area Managers have continued to focus their efforts on driving increased awareness and understanding in order to deliver improvements in conformance as BAU activity on branch visits and Teams calls. This has been underpinned with additional training where required and through frequent communications.

The latest mystery shop results described below, show performance levels for Inland continue to remain static ranging between 44% and 55%* with International between 65% and 90%*.
*number of branches correctly following the correct process based on mystery shopping

2020/21 YTD Mystery Shop Performance - periods 3:10
(N.B. limited P10 data due to cessation of Mystery Shopping mid-period)



11

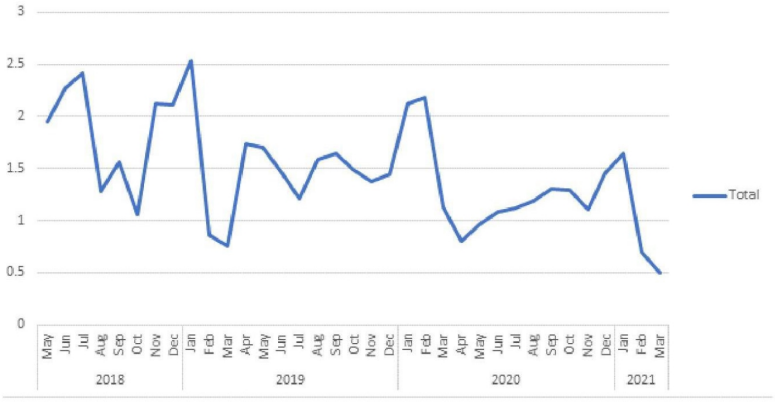
Confidential

POL00423695

The graph below shows the number of parcels disposed of per 100,000 items of mail accepted, as a result of the parcel containing a prohibited or restricted item. This data is provided by Royal Mail. This shows an improving trend year on year as follows:

2018/19	1.7 items disposed of per 100,000 items of mail
2019/20	1.6 items disposed of per 100,000 items of mail
2020/21 YTD	1.1 items disposed of per 100,000 items of mail (Period 11 0.6)

The target for 2021/22 is 0.5 items per 100,000 items, and we are confident that this will be achieved following on from the planned Horizon system updates. Area Managers will continue to make targeted interventions with branches using the Branch Insight Tool (BIT).



2. What is the impact of not doing this?

The Civil Aviation Authority may withdraw the authorisation of individual PO Branches to sell parcels in the event of non-compliance. The limitation of POL liability to an aggregate amount of £20 million per year – although POL has not to date received any claims for compensation from RMG for non-compliance with the MDA dangerous goods compliance requirements. In addition to this, there are reputational risks to the POL brand in the event of an incident occurring as a result of mail accepted in branch.

11

3. What steps have been implemented since the last ARC update (July 2020) to address this?

A meeting was held with RM and the CAA to discuss performance at the end of April, this was attended by senior members of the POL mails and network teams. POL and RM have continued their monthly Dangerous Goods working group to discuss performance and monitor improvement activities.

Following these meetings, and after several consultations with Postmasters during lockdown 1, there were a number of suggestions made for improvements. All improvements were scoped, prioritised and are being tracked in a project plan, some of which have already been implemented as part of phase 1 and some are in flight within phases 2 and 3. Following the implementation of each phase, we expect to see marked improvements across all Prohibited and Restricted metrics.

We are confident that the planned system changes described below, will drive a significant improvement in conformance as we are minimising risk by removing the reliance on the counter colleague to follow the correct process.

POL00423695

Phase One:

- Horizon System Changes - We will be able to offer a Horizon menu-based alternative to the manual scanning of the dangerous goods laminate. The Dangerous Goods process will be integral to the Mails transaction and will form a key part of the Mails conversation with customers without the need to use additional support aids such as the existing Dangerous Goods laminate. The current process relies on the colleague remembering to use the laminate. This new process is currently going through Network gateway for UAT testing and Postmaster feedback. We anticipate this will be going live in a trial capacity before the end of this financial year with the potential of a full roll-out across the entire network by the end of quarter one 2021/22.

(Accompanying this paper is a PDF document that demonstrates the changes from the existing to the new Horizon customer journey (appendix 1)).

- Branch Insight Tool (BIT) enhancements – The initial review in July 2020 identified the need for improved management information to support the identification of 'At Risk' branches. Following this review, from Q3 of last year, individual branches are now scored and ranked to prioritise those branches with significant non-conformance. This is based on overall Mails volumes, interception volumes, previous mystery shop results and Dangerous Goods laminate scan percentages. This development within the BIT tool, now provides Area Managers with improved visibility of overall performance across their areas. Looking forward, this will facilitate both reactive and pro-active actions to drive improvements in conformance.

4. What additional steps are planned to improve compliance further?

Phase Two (subject to CAA approval):

- Labels Compliance – We are working on a solution to enable the Horizon system to print both the ID8000 and Lithium battery label. Our worst performing mystery shop scenario is where these labels are required. Forcing the label to print during the transaction will drive further improvements in conformance by removing the option to add the label at a later stage. (Anticipated to go live is Q2 2021/22).

Phase Three (subject to business case):

- Simplification – We have requested a quote to update Horizon from our IT suppliers to see if we can move the DG transaction start point to earlier in the Post Mail items journey and will be subject to costings and appropriate finance approval.
- Customer Self-Confirmation – Further system changes are planned as part of phase 3 leading to a requirement for customers to confirm their self-declaration using Pin-Pad devices for Mails items. (Anticipated to go live Q2/Q3 2021).

5. What is the current focus in the network to address this?

The current focus in the network is as follows:

- Postmaster Engagement – The Horizon system changes, (described in phase 1) above, are now ready for testing and we have engaged with Postmasters to seek their input regarding the original needs analysis and whether the new system design will deliver against these needs.

Confidential

POL00423695

- Targeted Activity – Conformance Champions are in place across the 9 regions and they have been asked to lead regular sessions with their teams to increase focus and awareness across each area. Area Managers are now contacting their worst 20 branches based on zero scans of the Dangerous Goods laminate which highlights marginal/non-existent activity at the counter. This activity will continue ongoing which will lead to greater reach and positive impact across the network in the worst performing branches.

- Contractual Intervention – Work is progressing to agree and deploy a formal contractual process, where following three interventions and support provided by Area Managers, a branch continues to be non-conformant. We expect this to be in place by the beginning of the new financial year.

Conformance improvements expected

As a result of the anticipated Horizon improvements we expect to see a significant improvement in conformance to the process, as the necessary prompts and interventions are systems generated and will address current failure points.

For phase 1 we expect to see conformance improve as follows:

- Increase inland dangerous goods conformance to c.70%
- Increase international dangerous goods conformance c.85%

For phase 2 we anticipate conformance for inland and international dangerous goods conformance to improve to c.90%.

The anticipated improvements from the implementation of phase 3 changes would see conformance improvement to c.95% with the inclusion of customer confirmation.

Confidential

POL00423695

Appendix 1: Dangerous Goods Technical Improvements Phase 1 Horizon Menu based alternative to DG laminate

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Strategic Partner Financial Stability update	**Meeting Date:**	16 March 2021
Author:	Emma Conroy, Interim Head of Strategic Partnerships / Ed Dyer, Working Capital & Cash Management Lead	**Sponsor:**	Dan Zinner, Group Chief Operations Officer

Input Sought: Noting

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 Mar 20 and Nov 20

Executive Summary

1. At the ARC meeting Nov 20, discussion was held as to the rigour around the monitoring and tracking of Strategic Partners, the ask was to provide the committee with confidence that the business had a robust solution in place to support monitoring and mitigation of risk and to come back to you in May, we are on track in delivering this for the May committee.

2. This paper provides an update specifically on McColls where risk has been greater over the past 18 months. We update on the current trading position of McColls, where some positive news has been communicated in the last few weeks, and given previous concerns, this news should provide the business with some comfort around the stability of trading conditions within the McColls estate. Appendix 1 provides an updated Dashboard on McColls.

3. WHS has also been cited by the committee in similar regard by way of level of risk, no material change has been seen since the last update, albeit news in the last few days has been positive in terms of Jan & Feb trading vs PY performance up at 74% & 84% retrospectively. Interim HY results are due from WHS on 29 April, therefore we propose to provide a further update at the ARC meeting in May.

12

Questions addressed

4. What is the current financial status & risk to the most concerning of our strategic partner McColls?

Confidential

POL00423695

Report

What is the current financial status & risk to the most concerning of our strategic partner McColls?

McColls (status: AMBER)

5. McColls' preliminary results for the 53-week period ended 29 November 2020 are due to be published on 23 March 2021. The trading update published on 10 December 2020 pointed to adjusted EBITDA pre IFRS 16 of between £29m to £30m (FY19: £32.1m). Revenue growth of 2.3% has been offset by margin pressures driven by a change in shopping behaviours during the pandemic to deliver EBITDA lower than the previous financial year.

6. McColls continues to suffer from an overleveraged balance sheet, with a net debt to EBTIDA ratio of c.3.1x as at 29 November 2020.

7. Importantly, McColls announced support from its banking syndicate on 1 March 2021 which has agreed to amend McColls' facilities to offer improved headroom against covenants, a realigned amortisation schedule and an extended maturity date to February 2024. The updated facility consists of a £100m revolving credit facility and an amortising £67.5m term loan. This follows the sale of its head office for £7.3m in January 2021, which appears to have been a condition of the debt facilities restructure.

8. In the same update, McColls announced new terms with Morrisons to become the single wholesale supplier to the whole of the McColls estate until January 2027. The agreement also covers the conversion of 300 stores to the Morrisons Daily format over the next three years. Whilst McColls expects this to drive improved profitability, it raises its key partner risk.

9. The market reacted positively to the 1 March 2021 announcement with McColls' share price increasing from c.24p before to trading around c.31p as at 9 March 2021.

10. Prior to the extension of its banking facilities, Experian's reporting of supplier payments beyond terms showed McColls delay payments to suppliers on a growing basis from 63 days in February 2020 to 156 days by January 2021. This suggests cash conservation in order to comply with banking covenants. The support from McColls' banking syndicate should enable the business to improve payments to suppliers, which we will monitor over the coming months.

11. McColls continues to deliver against its closure plan announced last year which has seen the Post Office branches reduced from 608 to 522, with a view to this reducing to 456 by June 2021. We are currently collating with the network a RAG status report by partner of those locations that are critical / important / managable risk, to ensure we understand at any one time the level of critical risk within the partner estates.

12. In conclusion, the recent announcement from McColls is positive as it provides a period of stability to deliver against the turnaround plan. However, it is important that POL remains alive to the risk of failure given McColls overleveraged financial position which leaves it vulnerable to trading downsides or adverse shocks. We will continue to monitor McColls closely.

Confidential

POL00423695

Appendix 1
McColls risk overview & update

McColl's Red Flag Report: Mar-21

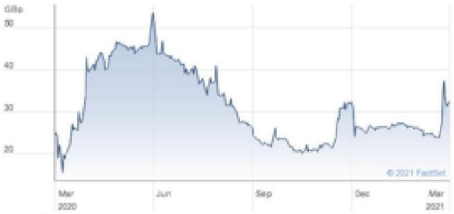
McColl's Retail Group plc		£m
Revenue	Nov-19	1,218.7
Operating Profit/(Loss)	Nov-19	(90.4)
Net Debt/EBITDA	Nov-20	3.1
Net assets	24-May-20	26.2
Market cap	09-Mar-21	35.2
Experian Delphi Score (out of 100)		60
Experian - Odds of Failure (next 12 months)		24:1
Value of outstanding CCJs		£3,772
Number of POL branches		522
POL Income YTD (£m)		25.6
POL Income YoY (%)		105%
POL Income YTD v Target (%)		107%

Year end: November
Interim period end: May

Red flags:

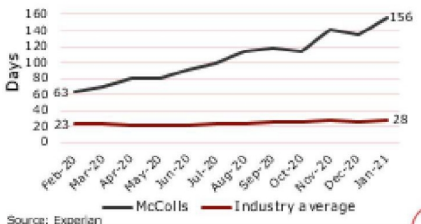
- Announced plans to close 300 stores in Feb-20 (including 152 PO branches).
- Bank debt of c.£168m is approx. 5.7x pre-IFRS 16 EBITDA of £29m-£30m, which is high relative to typical lending limits of 4x.
- Supplier payments being stretched (see graph below), suggesting cash flow pressures.
- Obtained support from its banking syndicate on 1 March 2021 to offer improved headroom against covenants, a realigned amortisation schedule and an extended maturity date to February 2024. The updated facility consists of a £100m revolving credit facility and an amortising £67.5m term loan. This follows the sale of its head office for £7.3m in January 2021, which appears to have been a condition of the debt facilities restructure.
- Delayed release of interim results from 14 July to 4 August (indication that something needed resolving).
- 4 of the 8 directors appointed in 12 months: Giles David (CFO), Richard Crampton (CCO), Benedict Smith (Non-Exec) and Dominic Lavelle (Non-Exec).
- Operating profit in y/e Nov-19 driven by £98.6m goodwill impairment.

1-year share price trend



Source: Hargreaves Lansdown

Supplier Payments Beyond Terms



Source: Experian

1

Post Office®

Post Office Limited – Commercial in Confidence

12

3

Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Procurement Governance & Compliance Report	**Meeting Date:**	16 March 2021
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 the Procurement Risk Exceptions submitted to the Post Office Limited Group Executive and Board since January 2020 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.

Previous Governance Oversight

- September 2020 – Board Report
- November 2020 – RCC & ARC Report
- January 2021 – RCC & ARC Report [no Board submission required]

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 submitted to the Group Executive for prior approval and 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.

Strictly Confidential

POL00423695

Questions addressed

1. *How many and what types of procurement risk exceptions have occurred in the past quarter?*

   Since the last RCC report at the end of January there have been two Procurement Risk Exceptions submitted to the Group Executive for approval.

   - NCR SSK Support – Interim extension of 30 days to 28.02.2021
   - NCR SSK Support – Interim extension of 30 days to 31.03.2021

   We also 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. This has not been resolved since the last RCC report in January.

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, £9.2m in November and is now £7.7m.

   A visual breakdown on all Open incidents at 5/03/2021 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 number of Procurement Risk Exceptions will be submitted for GE review and onwards to Board in March if approved.

   a) **£100-150k pa. Cheque Processing for Postal Orders and Camelot**.

      The Corporate Banking Services contract expires in March 2022 and is due to be retendered in Q3 2021. There are operational consequences for Post Office should we split the services across two banks and so Procurement are proposing to extend clearing for Postal Orders and Camelot cheques and include into the scope of the Corporate Banking Contract. Subject to GE approval a decision has been taken to amalgamate these two services. An interim extension will be put in place while a tender process is completed in Q2 of FY 2021/22.

   b) **Lexington Communications – Circa £500k.**

      The PR&Comms team wish to extend the existing non-compliant contract [£173k] with Lexington Communications out to September 2021 in order to cover immediate business requirements relating to GLO.

Strictly Confidential

POL00423695

Aggregated value is forecast at circa £500k to September 2021.

c) **Digidentity – TBC**

Contract and settlement negotiations with Digidentity are continuing. A full commercial overview and risk analysis will go to GE and Board in due course, noting that by accepting a non-compliant extension from GDS, and therefore, commercially entering into an extension with Digidentity to provide the services, a Procurement Risk exception must be considered and approved.

Conclusion

Risk Exceptions are subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk. This is reflected in the material reduction in the value of open risks over the past 3 years.

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

4. 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.

5. Why are these incidents of non-compliance occurring, and what can be done about it?

   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

Strictly Confidential

POL00423695

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.

6. 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.

7. 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.

8. 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.

9. Why were the approvals given?
The rationale for approval is relevant to the individual service and is detailed within Appendix 1.

10. What were the unapproved, material breaches?
There were no unapproved, material breaches during this period.

Strictly Confidential

POL00423695

11. 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.

Risk Assessment, Mitigations & Legal Implications

12. 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.

13. 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,

POL00423695

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.

14. 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.

15. 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.

POL00423695

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.
23/12/2019	PR	Corporate Affairs & Comms	Richard Taylor	Cardew Group	£ 377,860.60	Pending	PCR OJEU level	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	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 due to Covid19. Completion due March 2021
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
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
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

Strictly Confidential

POL00423695

Date	Procurement Category	Function	GE Member	Supplier Name	Value	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
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	£ 200,000.00	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
11/11/2020	Professional Services	Finance	Alisdair Cameron	Smith & Williamson	£ 150,000.00	None	Medium threshold	Board requested additional professional advice support to form an independent view of the way in which the Group's funding agreements, financing arrangements, headroom limits, cross-defaults, commercial contract implications and net liability exceptions (the "Facilities") have been forecast
16/12/2020	Professional Services	Commercial	Owen Woodley	Grant Thornton	£ 125,000.00	None	Medium threshold	Urgent financial support required in relation to HPBB sale
					£ 8,906,018.81			
					£ 7,706,018.81	excluding Audit Value		

Strictly Confidential

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	16th March 2021
Author:	Reena Chohan People and Policy Compliance Manager	**Sponsor:**	Jonathan Hill, Director of Compliance / Ben Foat, Group General Counsel

Input Sought: Approval

The Committee is asked to review and approve the following policies:

i. Health & Safety Policy; and
ii. Procurement Policy

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

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?
3. What is Compliance's assurance view of the status / Minimum Controls Standards for each policy?

Which Group policies were updated in this annual cycle review?

In this review cycle the following group policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Sponsor	Governance Approval Body
Health & Safety Policy	April 2020	Updated into policy format	Group Chief Finance Officer	RCC & ARC
Procurement Policy	July 2020	Regulation update due to Brexit and changes to the Risk Exception Process which were proposed after the ARC meeting in Sept 2020.	Group Chief Finance Officer	RCC & ARC
Whistleblowing Policy	July 2020	To be discussed in a separate paper by Sally Smith.	Group General Counsel	RCC & ARC

14.1

POL00423695

What updates were included and why?

A summary that identifies the changes and updates to the policies and statements have been added below:

Health & Safety Policy: The policy does not contain major changes, but it has for the first time been written into the Group policy format, including the required minimum control standards. The operating practices in Appendix A are what was included as the 'policy' previously.

Policy Compliance View

The minimum control standards whilst 'new' are based on well-established Post Office processes. Compliance has not had a chance to test these. But bearing in mind the COVID-19 health emergency it would be prudent to test whether these practices and controls worked.

Procurement Policy: Brexit has altered the regulations, therefore the policy, the procurement manual and the P-suite of contracts have been amended to bring them up to date and in line with the correct terminology. Further changes have been made to the Policy post ARC approval which took place in Sept 2020, the areas updated in the policy include:

a) Risk Exception;
b) The removal of Appendix A within the policy;
c) The compliance section and application section of the policy.

Given the above changes and updates to the policy which are subject to governance, full re approval of the policy is being sought from both the Risk & Compliance Committee and the Audit, Risk & Compliance Committee.

Whistleblowing Policy: To be discussed in a separate paper submitted by Sally Smith (MLRO)

Postmaster Policies: To be discussed and approved in a separate paper, presented to the Committee by Tim Perkins (Service and Support Optimization Director).

Approval is being sought on a further set of postmaster policies. This include policies dealing with postmaster complaint handling, management of cash & stock in the network, issuing of transaction corrections and how a postmaster appeals a decision to terminate their agreement. Full summaries are provided in the Postmaster Policies submission document.

Assurance

Working with the Policy Owner of the Conflicts of Interest Policy we have now completed the pilot assurance process and sample test of the policy on a risk basis to review the policy standard and policy compliance. We reviewed a sample check of 4 Minimum Control Standards stated within the policy *(Gifts and Hospitality, Reporting, Incentive Payments and Training & Competence).* This included:

POL00423695

- A sample check of any relevant registers to ensure any breaches/conflicts of interests have been identified, disclosed and effectively managed.
- A review and sample check to see if the business has complied with the relevant legal and regulatory requirements stated in the policy *(in this review the assurance was based upon the Public Contract Regulations 2015)*
- Sample testing the process for identifying, disclosing and managing conflicts of interest and how transparent it is.
- Sample testing how clear the guidance is around how to report conflicts of interest or concerns related to them.

The overall review of the above-mentioned control standards and regulation within the COI Policy, confirmed that they are deemed as fit for purpose and working with a few minor gaps identified, which relate to minor control weaknesses or process inefficiencies. The gaps have been addressed within the report, which is currently being reviewed by the policy owner and CoSec, compliance are awaiting feedback and approval.

Other Developments

The Internal Policy Template which is used by policy owners to draft their policies on has now been finalised to reflect current working practices as the previous one was outdated. The new template now includes guidance notes for policy owners, to help assist them in writing their policies. This is to ensure we have a consistent approach to policies been written and aligned in the same format throughout the Group. The template and guidance notes have been uploaded to the policy hub on the intranet.

Whilst for the first time in a while we have a group policy suite that is current, up to date, owned and approved we are working with both the Company Secretary and the Chair of the Audit Committee on refining this list and ensuring the appropriate level of governance approval as the business and its controls evolve.

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.

POL00423695

Appendices

1. Health & Safety Policy (New format)
2. Health & Safety Policy (Previous version 2020)
3. Procurement Policy (Clean)
4. Procurement Policy (Track changed)

Please see separate paper for the Whistleblowing Policy and Postmaster Policies.

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Postmaster Policies	**Meeting Date:**	16 March 2021
Author:	Tim Perkins, Service and Support Optimisation Director	**Sponsor:**	Amanda Jones, Retail and Franchise Network Director Reviewed & approved by sponsor for presentation to the Committee.

Input Sought: Decision

The Committee is asked to approve the six new Postmaster policies (set out in the Appendices), for onward submission to the Audit, Risk & Compliance Committee (ARC) and to be effective from the date of ARC's approval:

- Postmaster Complaint Handling Policy
- Network Transaction Corrections Policy
- Network Cash and Stock Management Policy
- Postmaster Termination Decision Review Policy
- Postmaster Onboarding Policy
- Postmaster Training Policy

The Committee is asked to separately approve the issuing of a policy guide for postmasters (also set out in the Appendices), considering the legal advice, for onward submission to the ARC and to be issued from a date to be confirmed after ARC's approval:

- Postmaster Guide to Policies

Executive Summary

Following the Group Litigation Order (GLO), Post Office set about ensuring that its processes complied with the findings of the GLO.

The focus on processes delivered a large number of changes to the support that Post Office offers postmasters but these processes were not necessarily governed by a policy at the point of process changes being made. Primarily this was the case because no policy existed in the first instance or the policy was so dated that it was irrelevant to the processes undertaken pre or post the GLO.

Having policies in place for the support Post Office provides postmasters will bring Post Office in line with best practice franchise businesses. The purposes of the policies are to provide guidance, set down principles and highlight risk areas, while also ensuring that Post Office is able to support postmasters effectively and compliantly with the GLO.

As part of an overall review of postmaster support policy requirements, this paper seeks approval for four new postmaster policies to reflect how Post Office will provide support to postmasters as well as a guide to policies that will be made available to postmasters.

15

Internal

POL00423695

Questions addressed

1. What policies are required to support the changes made to postmaster support following the GLO?
2. What policies have recently been developed and now require approval?
3. What further policy work is required to ensure there is a full complement of postmaster support policies in place and how will these be continually reviewed in the future?

Report

Background

1. Following the Common Issues Judgment and Horizon Issues Judgment in the GLO, Post Office focused on improving processes to ensure compliance with the outcomes of the judgments.
2. Whilst process improvements were delivered, Post Office has identified that there was an absence of overarching policies for these processes to sit under. Where policies previously existed, they were often very aged and did not bear relevance to the processes that Post Office had improved.
3. As such, Post Office has set about developing a set of postmaster policies across key areas of postmaster support.

Postmaster Policies

4. Post Office has identified that a comprehensive suite of postmaster policies is required to demonstrate and ensure GLO compliant support to postmasters in the following areas:
    - Network Monitoring and Audit Support
    - Network Cash and Stock Management
    - Network Transaction Corrections
    - Postmaster Account Support
    - Postmaster Accounting Dispute Resolution
    - Postmaster Contractual Performance
    - Postmaster Suspension
    - Postmaster Termination
    - Postmaster Termination Decision Review
    - Postmaster Complaint Handling
    - Postmaster Training
    - Postmaster Onboarding
5. The policies relating to Network Monitoring and Audit Support, Postmaster Account Support, Contractual Performance, Postmaster Suspension and Postmaster Termination are already approved and in use.
6. The policy relating to Postmaster Accounting Dispute Resolution is ready for ARC approval by written resolution following offline reviewing with members of the ARC and legal.
7. This paper seeks approval of the policies relating to Postmaster Complaint Handling, Network Transaction Corrections, Network Cash and Stock Management, Postmaster Termination Decision Review, Postmaster Onboarding and Postmaster Training. These policies can be found in the appendices to this paper.
8. This paper also seeks approval of the Postmaster Guide to Policies which can be shared with postmasters. This document can also be found in the appendices to this paper.

POL00423695

9. Previous papers to the RCC and ARC indicated that a Postmaster Accountability policy would also be developed. Following a review of the requirements for this particular policy, the requirement for such a policy has been de-scoped.
10. All policies and the policy guide have been reviewed by Post Office internal stakeholders, the National Federation of Subpostmasters (NFSP) and have had external legal oversight from Herbert Smith Freehills or Norton Rose Fulbright.

Policy Overviews

11. The Postmaster Complaint Handling policy sets out the standards relating to the management of postmaster complaints, that a fair process is followed for all postmaster complaints and that any complaint raised is taken seriously and investigated fully. It also gives guidance on the identification of whistleblowing reports.
12. The Network Transaction Corrections policy details the standards behind how Post Office identifies and issues Transaction Corrections and Transaction Acknowledgements, ensuring that postmasters are notified without undue delay and that support is provided to understand the reasons behind the issuing.
13. The Network Cash and Stock Management explains the principles to ensure that postmasters are supported effectively in managing cash and stock provisions in branch.
14. The Postmaster Termination Decision Review policy sets out how Post Office will deal with any situation whereby a postmaster does not agree with a decision to terminate their agreement, either by notice or immediately.
15. The Postmaster Onboarding policy details the principles that ensure that new postmasters are supported effectively in their early days, ensuring that the onboarding process meets regulatory and contractual obligations.
16. The Postmaster Training policy sets out the standards for ensuring that postmasters receive a comprehensive training provision to support the effective running of their branch(es).

Postmaster Guide to Policies

17. The Postmaster Guide to Policies is a document that can be shared with postmasters and is a guide to the principles that Post Office teams need to follow and how these principles are linked to specific policies.
18. A legal review of this document has identified some legal risks in the publication of this document. These are:
    - That the guide is not necessarily required from a good faith perspective;
    - That postmasters may consider the contents of the guide to be obligations of Post Office – and that the guide will make it easier for postmasters to claim that Post Office has not complied with its obligations under the guide or the policies themselves;
    - That Post Office's obligations under the guide go further than its contractual obligations; and
    - That it will be difficult to maintain the confidentiality of the internal policies as a result of the publication of the guide.
19. These risks have been mitigated to some extent by including wording in the guide and each policy to state that they do not form part of the contract with postmasters, and through ensuring that the guide will not be issued to postmasters prior to them entering into a contract with Post Office.
20. These risks should also be taken in perspective with Post Office's desire to provide reassurance to postmasters that Post Office has robust policies in relation to postmaster support following the GLO and its desire to be transparent in its dealings with postmasters.

POL00423695

Next Steps & Timelines

21. Following approval of the six policies, Post Office will ensure that:
    - all relevant teams are fully trained on the new policies by the end of April 2021.
    - the policies will be reviewed annually, for approval at RCC, beginning April 2022.
22. Policies previously approved at RCC and ARC in 2020 and 2021, will be updated and resubmitted with a list of changes at the RCC meeting to take place on the 4th May 2021, in line with the annual review requirements of the policies.
23. Following approval of the policy guide, Post Office will ensure that:
    - the guide is published to postmasters in line with the re-issue of the Postmaster Support Guide.
    - the guide is made available for postmasters to access online.
    - the guide will be reviewed annually in line with policy approvals at RCC, beginning April 2022.

POL00423695

Appendices

1. Postmaster Complaint Handling Policy
2. Network Transaction Corrections Policy
3. Network Cash and Stock Management Policy
4. Postmaster Termination Decision Review Policy
5. Postmaster Onboarding Policy
6. Postmaster Training Policy
7. Postmaster Guide to Policies

POL00423695

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Whistleblowing Policy Review & Report	**Meeting Date:**	16th March 2021
Author:	Sally Smith	**Sponsor:**	Ben Foat

Input Sought: Discussion & Approval

The Committee is asked to:

- review and discuss the whistleblowing review and its conclusions as part of its role in monitoring the adequacy and effectiveness of the Group's whistleblowing systems and controls; and
- approve the proposed amendments to the whistleblowing policy and the appointment of the Whistleblowing Champion.

Previous Governance Oversight

Annual Whistleblowing report and policy review July 2020.

Executive Summary

Post Office is able to demonstrate that it has good policies and procedures in place which have been followed. The preliminary view is that there is no evidence of detriment to whistleblowing reporters. This is based on an analysis of certain whistleblowing records performed by a lawyer from Herbert Smith Freehills LLP (HSF) working with the Whistleblowing Team. We are continuing our work with HSF to form a concluded view on this before the Audit and Risk Committee later in March. Whistleblowing engagement including training needs particular attention, together with operational improvements which are being addressed in April and May 2021.

As a result of the review of whistleblowing policy, processes and culture, there are a number of recommended enhancements to improve and mature these areas, including the creation of a Non-Executive Board Director Whistleblowing Champion.

Questions addressed

1. Are the current whistleblowing arrangements adequate in light of the GLO and the Public Inquiry?
2. Is there any evidence of detriment to whistleblower reporters or subjects?
3. What improvements are required to enable anyone who is aware of, or suspects, wrongdoing which affects others (e.g. Postmasters, customers, members of the public, colleagues or the Post Office) to raise their concerns and be confident that those concerns will be acted upon

POL00423695

Report

4. A number of improvements have been implemented since 2017, these include:

   - Enhancing Post Office policy and procedures, including attendance by whistleblowing team at industry forums to learn best practice
   - Raising awareness through communications and posters (which in turn has led to an increase in reports received)
   - Developing monthly MI and providing to key stakeholders
   - Regular reporting to RCC and ARC, including an annual whistleblowing report which summarises all whistleblowing reports received over the previous 12 months, compared to the prior 12 months. This report also details any issues or outcomes, together with key activities delivered to drive reporting

   However, it was recognised that more could be done to improve the maturity of the Post Office approach and as part of the review of this, Post Office approached Protect (the UK whistleblowing charity) for support. This has included a self-assessment and industry benchmarking of the regulatory requirements, current industry best practice and Protect's Code of Practice on effective whistleblowing arrangements, and a training workshop which was attended by some GE members and senior managers.

5. A review of high-level summaries of the 163 whistleblowing reports and investigations received since 2013 was undertaken to identify if there was any evidence of 'detriment' to reporters and specifically Postmasters. These cases were also considered, at a high level, for conformance to Post Office's obligations arising from the Common Issues Judgment from the GLO. The preliminary view from this review (summarised in Appendix 1) is that there have been no instances where detriment to a reporter has been suffered, although there are 15 cases where it was alleged, or could potentially have been suffered by the subject of the report. There are also 9 cases which are being further considered for conformance to the Common Issues Judgment in connection with suspension pay, although the suspensions appear to be justified by the circumstances. We are working with HSF to reach a concluded view on these matters before the ARC.

6. The monthly MI pack produced on whistleblowing has been updated to provide more granular data on issues that are raised by or about Postmasters.

7. As part of the work reviewing Postmasters complaints and issues handling, a review has also been undertaken to ensure that there is sufficient understanding across teams that interact with and capture those complaints and issues, so that any that are in fact whistleblowing reports are passed to the Whistleblowing Team and investigated and resolved in accordance with the whistleblowing policy.

8 [redacted]

   It is agreed that we should have a dedicated Whistleblowing Manager within the Compliance Team to manage whistleblowing but also to assist in the conduct of investigations. In addition, an approach was made to the ARC Chair to discuss creating a Whistleblowing Champion at Non-Executive Director level, following which Zarin Patel has been asked to fulfil this role, and has agreed, subject to RCC and ARC approval.

POL00423695

9. Following migration of the external speak up line and website to the new Navex Global EthicsPoint platform, call enhancements have been implemented to include an IVM that is specific to Post Office and provides reassurance to callers as below:

    - Thank you for calling the Post Office Whistleblowing Speak Up line. Post Office is committed to ethical behaviour in all our business dealings and your call and any related reports will be treated confidentially and respectfully to the extent legally permissible. Protecting our colleagues, Postmasters and customers is the number one priority for Post Office, and this includes protecting those that raise concerns. To maximize confidentiality, this Speak Up line is operated by NAVEX Global, an unaffiliated, third-party service provider.

10. To address the lack of formal training, a new module is being developed in Success Factors and will be rolled out to all employees on 15 March 2020 for completion by 1st April 2020, together with a number of communications for employees and Postmasters to raise awareness.

Self-assessment and benchmarking

11. The outcome of the Protect self-assessment and industry benchmarking was in line with expectations given that the benchmark is modelled around best practice and the bar is deliberately set very high.
12. Post Office achieved a score of 86% for its written policy and procedures and there were no specific recommendations, indicating that the basic foundations put Post Office in a good place to improve.
13. It was in the areas of training, engagement and communications that further work was identified.
14. The need for formal training and awareness in Post Office had already been recognised, with budget to develop a training module included in 2020/21.
15. The table below shows the overall performance of Post Office v. organisations with a comparable number of employees and also within the financial services sector which has a more mature approach to whistleblowing, given the additional regulatory obligations for this sector (see Appendix 2 for scores within these overall areas):

Total	Your Score	Group
Governance	72%	67%
Engagement	24%	39%
Operations	36%	55%
Total	46%	60%

- It should be noted that nearly all organisations come out very poorly for Engagement the first time they do self-assessment – this is because the main resolution for this area is training which is generally costly, and most often not seen as a priority. Usually selected people and teams have some form of training, but not enough and not company-wide. Also, there is a heavy score weighting for Line Manager training, and this is an area that Post Office was unable to demonstrate.
- Organisations also tend to score poorly in the area of Operations and there are a number of factors here:

POL00423695

- Whistleblowing process maturity tends to reflect the cases organisations have had to deal with – if an organisation has not had any cases that are material/significant, or had whistleblowing reporter claims of detriment, then they are less likely to have matured their processes.
- Included in this area are questions about seeking feedback from whistleblowers about their experiences or doing 'tests' or 'stress tests' of the whistleblowing processes – most organisations do not do this, but it is best practice.

- A number of organisations re-run the self-assessment and benchmarking exercise annually to help them demonstrate continuous improvement as part of their Board reporting which means the benchmark is continually rising as organisations improve. We will re-run the self-assessment in June 2020 (and annually thereafter) following the implementation of planned enhancements to show how Post Office is building on its improvements.

Whistleblowing Policy Review

16. In addition to further enhancements suggested by the Protect self-assessment work and the changes to whistleblowing roles, a comprehensive review of the Whistleblowing policy, alongside the Investigations and Postmaster Complaints policies has been undertaken by HSF. A review of the BEIS Guidance and Code of Practices for Employers published in March 2015 was also undertaken. A number of enhancements have been incorporated and are summarised below.

17. The policy has been amended to reflect the following new roles and governance oversight:

- The creation of a Non-Executive Director Whistleblowing Champion to oversee that:
  - A 'whistleblowing culture' is promoted across Post Office, ensuring employees are genuinely encouraged to speak openly and honestly about their concerns and misgivings
  - The current arrangements are always challenged and assessed for areas of continuous improvement
  - Employees are always supported in raising a concern
  - Barriers to speaking up are uncovered and addressed
  - The whistleblowing team, senior managers and leaders receive training on the importance of whistleblower support
  - Root cause analysis is undertaken for all cases and issues, so that continual improvements can be made in the relevant areas
- The creation of a new dedicated Whistleblowing Manager to manage whistleblowing processes and investigations, triaging reports and assigning to investigating managers, completing root cause analysis and ensuring any corrective controls are implemented, designing and delivering a programme of training and awareness

18. A number of amendments and additions have been made to reflect best practice, enhance the policy and help encourage reporting. These include:

- Removal of some duplication and clarifying the definition of whistleblowing, the investigations process and the treatment of reporters
- Providing more information to reporters (e.g. other external advice available)
- Clarification of some of the definitions used in the policy

POL00423695

- Clarification that reporters do not need to provide evidence and the different reporting types along with the benefits and disadvantages of open/confidential/anonymous reporting
- A new minimum control standard for line managers.
- A new minimum control standard for checking that whistleblowers feel supported

Conclusions and Recommendations

19. Post Office has a good policy and reports received have been managed in accordance with that policy, although clearly further work on engagement including training together with operational improvements are needed and are being quickly remediated Whilst the policy and process were intended to cover employees and the protections afforded them under the law, reports have historically been received from postmasters, their teams, customers and the general public, and these reports have always been investigated and managed under the whistleblowing policy. Improvements to communications and awareness have been made in recent years, but the lack of training for all employees and, in particular, line managers needs addressing.
20. The work with Protect has highlighted that whistleblowing process maturity tends to reflect the cases organisations have had to deal with. To date, Post Office has not had any material reports, or found evidence of significant or material (or disclosable) wrongdoing through the whistleblowing channel. By quickly implementing the recommendations within this report, management believes that it would put Post Office in a good place.
21. Prior to the Protect self-assessment, it had been recognised that a training and communications programme was required in 2020/21 and this was budgeted for, although this was hampered by Covid, and the loss of the role supporting this work in November 2020.
22. The following lists the recommended activities to be delivered in 2021/22 (see Appendix 3 for full actions and timescales):
    - Continue to work with Protect to identify improvements and enhancements
    - Provide the monthly whistleblowing MI pack to all GE members to ensure visibility
    - Quarterly meetings with the Whistleblowing Champion to review cases and activities, together with monthly meetings with the postmaster and customer complaints teams to ensure that complaints or issues they receive that are in fact whistleblowing, are appropriately identified and investigated.
    - Work with the People Function and L&D to enhance on-boarding and line manager training relating to whistleblowing
    - Review and update the Whistleblowing Team's procedures, including those relating to the whistleblower and mechanisms to obtain feedback from whistleblowers
    - A programme of continual communication and awareness, including refreshing posters for office locations as staff return to work locations following Covid
    - Update Settlement Agreements to remove potential ambiguity
    - The Protect self-assessment benchmarking should be undertaken again in June 2021 and annually thereafter to test and demonstrate improvements achieved from planned activities

POL00423695

Appendix 1 – Whistleblowing Report Review

Number of Whistleblowing Records Reviewed (From 25/04/2013 to 25/01/2021)	**163**
REVIEW FOR DETRIMENT	
Number of cases ongoing (no apparent detriment and no CIJ breaches identified in investigation of complaint to date).	*6*
Number of historic cases where information is insufficient for assessment *These predate whistleblowing falling under the remit of the Financial Crime Team. The most recent record is 23.09.2017*	*9*
Number of Whistleblowing Reports NOT within Scope of the Whistleblowing Policy • *Employment matters between Postmaster and the Postmaster's employees: 5* • *Properly dealt with outside of Whistleblowing channels e.g. dignity at work: 11* • *Properly referred to external organisations such as RMG: 5* • *Other cases which did not meet WB criteria (These cases are quite varied but include for example, PMs are calling for advice from the Security team; a report raised by a known individual harassing branch staff, and errors/mistakes relating to applications for hardship grants): 9*	*30*
Number of Whistleblowing Reports WITHIN scope of the Whistleblowing Policy • *No detriment suffered by the Reporter, the Subject or anyone associated with the Report: 103, including* ○ 6 cases where inadequacies with POL's policies and procedures alleged but where no specific detriment to an individual identified (for example, two complaints related to the same alleged incident of sexual harassment which took place outside of POL premises. The reporters were not the victim of the alleged incident; one of the POL managers was present at the time and the reporters were concerned that the manager didn't take any action/ provide support when the alleged victim returned to work. HR could not investigate any further due to lack of information). ○ 1 case where reporter withdrew complaint due to slow response time. The Reporter was subject to a grievance which was raised by the Subject of the WB report. Legal advised the WB disclosure should be investigated subsequent to the grievance being heard. The POL employee who was due to investigate the WB disclosure left the business without informing the WB team which caused delays. The WB team did contact the Reporter to encourage them to pursue the case, but did not receive any response. • *Detriment suffered by the Subject, with Detriment justified based upon evidence and rationale: 15* ○ 12 cases where PMs have been suspended and/or terminated due to ongoing operation issues. ○ 2 cases where the agent assistant/clerk was dismissed by the PM for suspected/admitted theft. ○ 1 case there were formal consequences for the Branch Manager, which were justified upon investigation. In addition, in this case, the Subject was said to have obtained copies of witness statements which, had the WB disclosure not been made anonymously, could have compromised the Reporter's identity. Enquiries were made but these were not able to determine how or if the witness statements had been shared with the Subject.	*118*
CIJ CONFORMANCE REVIEW	
CIJ Issues NOT relevant	142

CONFIDENTIAL

Post Office Limited - Risk and Compliance Committee-16/03/21

POL00423695

CIJ Issues ARE relevant: 21 (including 1 case still ongoing) ○ Dealt with in a GLO conformant Manner: 12 (including 1 case still ongoing) ○ Not dealt with in a GLO Conformant Manner: 9 - While suspensions appear to be justified by the circumstances, the PMs were suspended without pay (predates the CIJ).	21

Post Office Limited - Risk and Compliance Committee-16/03/21

CONFIDENTIAL

POL00423695

Appendix 2 – Protect Review Recommendations

Section	Score
Accountability	61%
Written Policy and Procedures	86%
Review and Reporting	59%
Total	72%

Accountability – 61% Considers the roles different individuals have and their engagement with the whistleblowing arrangements. Clear accountability structures will help staff better understand their roles in relation to the whistleblowing arrangements. Active engagement from senior leaders may improve staff trust and confidence in your whistleblowing arrangements.

Recommendation - You have a good score in this area. In order to improve on this score in line with best practice, you need to show how senior leaders within your organisation engage with the whistleblowing arrangements and actively demonstrate a commitment to workers raising concerns without fear of reprisal. You also need to ensure that designated personnel (for example the whistleblowing champion and team) clearly understand their roles and responsibilities.

Written Policy & Procedures – 86% A well drafted whistleblowing policy helps to provide staff with a clear understanding of what whistleblowing is and the processes by which an individual can raise and/or escalate a concern. It will also provide staff with assurances about victimisation and confidentiality

Recommendation - You have achieved a good score in this area and there are no specific recommendations at this stage

Review & Reporting – 59% Considers the processes by which you review and report on whistleblowing arrangements. Conducting reviews enables organisations to practically see whether whistleblowing arrangements are effective in practice and action learning points.

Recommendation - You have achieved a good score in this area, but additional work should be considered to strengthen governance. When reviewing the arrangements, recommendations should be assigned ownership with a timeline for completion. Serious concerns raised and positive outcomes from whistleblowing cases should be reported to the Board. These should be redacted in order to protect the identity of the whistleblower. You could consider incorporating an overview of management information on whistleblowing in published data e.g. annual reports.

POL00423695

Section	Score
Communications	30%
Training	8%
Total	24%

Communications - 30% Engaging regularly with staff is essential to building a strong speak up culture. Staff will not have confidence in whistleblowing arrangements if they are not aware of them.

Recommendation - This section requires improvement. We recommend that you review your communications materials to ensure that you engage with different staff groups and cultures. Messages encouraging staff to raise concerns might be included in various media such as posters and staff training. Finally, think about how you test staff awareness and confidence in the whistleblowing arrangements (for example by using staff surveys, focus groups and exit interviews)

Training – 8% Clear and detailed training on whistleblowing provides your workforce with a good understanding of arrangements. Training can help embed the importance of whistleblowing and key policy messages.

Recommendation - This section requires improvement. We recommend that staff, designated managers and line managers receive in-depth training on whistleblowing. In most circumstances line managers or named designated contacts are the first people to receive a whistleblowing concern. Accordingly, line managers should receive appropriate training in order to accurately identify concerns and effectively handle the individual raising the concern. This minimises the likelihood that concerns will be escalated further and helps make best use of your resources. You may wish to review how you provide training to your workforce (e.g. instructor led by e-learning).

Section	Score
Support and Protection	41%
Recording and Investigations	56%
Resolution and Feedback	18%
Total	36%

Support & Protection – 41% Considers internal processes in place for supporting and protecting staff who raise whistleblowing concerns. Implementing effective processes for managing confidentiality and victimisation will help to ensure staff are appropriately supported and protected when they raise concerns. Implementing clear policy messaging and protocols for supporting and protecting staff who raise concerns is essential.

Recommendation - This section requires improvement. We recommend that you operate multiple support networks within your organisation to enable whistleblowers to seek support when raising concerns (such as whistleblowing advocates trade unions and Employee

POL00423695

Assistance Programs). Consider how you ensure that confidentiality is maintained throughout the whistleblowing process. You should ensure the risk of victimisation is considered in each whistleblowing case and that appropriate safeguards are put in place to prevent this. Finally, you should ensure that any settlement agreement that you have with staff clearly states that nothing in the agreement prevents staff from making a whistleblowing disclosure.

Recording & Investigations – 56% This section considers the processes by which you record and investigate concerns. Having clear processes and principles for recording and investigating concerns will help to ensure consistency in handling a whistleblower.

Recommendation - You have achieved a good score in this area. We recommend that you periodically review management information to ensure consistency of processes in recording concerns. You should ensure that investigation guidance is clear on the key principles that are to be followed when whistleblowing concerns are investigated (such as confidentiality, competence and independence). You should ensure that an independent internal function conducts periodic reviews of your investigations, to ensure that the principles have been followed.

Resolution & Feedback – 18% This looks at your processes for resolving concerns and how you provide feed receiving feedback from whistleblowers. Clear processes on feedback after the investigation will help give your staff confidence that their concerns have been addressed.

Recommendation - This section requires improvement. We recommend that you implement standard processes for resolving any substantiated concerns. Where possible ensure that you provide feedback to whistleblowers on the outcome of concerns that are raised (subject to limitations imposed by confidentiality). Consider how you seek feedback from whistleblowers at the end of the process and use this information to improve your arrangements.

POL00423695

Appendix 3 – Whistleblowing Action Timetable

Action	By when	Status
Protect training workshop	January	Complete
Review how complaints are captured by various back office teams and enhance procedures to correctly triage potential whistleblowing complaints and pass to whistleblowing team	February	Complete
Design and deliver employee survey via One Comm (440 responses fed into Protect self-assessment)	February	Complete
Enhanced Whistleblowing monthly MI to provide more granular detail about Postmaster/agent assistant reports	February	Complete
Protect self-assessment and benchmarking	February	Complete
Review all historic whistleblowing reports	February	Complete
Whistleblowing Manager role designed, approved and advertised	February	Complete
Whistleblowing Champion role approved in principle	February	Complete
Navex Global Speak Up Line - call enhancements to include IVM that is specific to Post Office and provides reassurance to callers	February	Complete
Review and update Whistleblowing Policy	March	Complete
Determine whether there is any evidence of detriment to whistleblower reporters or subjects	March	In progress
RCC and ARC whistleblowing approach and policy approval	March	Pending
Interviews for new Whistleblowing Manager role and recruitment	End April	In Progress
Design and deliver new employee Success Factors whistleblowing training module	1st April	In progress
Design and deliver new Team Talk whistleblowing training module for DMB staff and Supply Chain (non-Success Factor users)	1st April	In progress
Design and deliver postmaster whistleblowing awareness communications	April	In progress
Establish monthly meetings with the postmaster and customer complaints teams to review complaints or issues	April	
Training and induction for Whistleblowing Manger	May	
Design a programme of continual communication and awareness	May	
Establish quarterly meetings with Whistleblowing Champion	May	
Design and deliver employee survey via One Comm	May	
Review and update all whistleblowing processes and guidelines	May	
Re-run Protect self-assessment benchmarking	June	
Annual whistleblowing report to RCC and ARC	July	
Enhance on-boarding and line manager training relating to whistleblowing	July	

POL00423695

Refresh and deliver new whistleblowing posters to all Post Office back office locations and DMBs	July (dependent on Covid)	

POL00423695

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	30 March 2021
Time:	09.00 – 11.30
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Alison Rodwell (BEIS ARAC NED Observer)
Ken McCall (SID)	Tim Perkins (Service and Support Optimisation Director): Item 2
Tom Cooper (NED, UKGI)	Sally Smith (Money Laundering Reporting Officer & Head of Financial Crime): Item 3
Zarin Patel (NED)	Amanda Bowe (Post Office Insurance ARC Chair): Item 7
Regular Attendees:	Jonny Lonsdale (Business Continuity Manager): Item 8
Tim Parker (Group Chairman, POL)	Martin Hopcroft (Head of Health & Safety): Item 8
Nick Read (Group CEO)	Andrew Goddard (Managing Director, Payzone): Item 9
Alisdair Cameron (Group CFO)	Andy Kingham (Franchise Partnering Director): Item 10
Ben Foat (Group General Counsel)	Mark Siviter (Product Portfolio Director – Mails, Retail, PUDO & Gov services): Item 10
Andrew Paynter (Audit Partner, PwC)	
Sarah Allen (Senior Manager, PwC)	
Rosie Clifton (Manager, PwC)	
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
Rebecca Whibley (Senior Assistant Company Secretary)	
Hugo Sharp (Deloitte Partner)	

Join Microsoft Teams Meeting
GRO United Kingdom, London (Toll)
Conference ID: 908 090 140#
Pin (if applicable): 58042

Time		Item		Owner	Action
09.00	1.	Welcome & Conflicts of Interest		Chair	Noting
09.05	2.	Postmaster Policies		Tim Perkins	Approval
		2.1	Guide to Policy Standards for Postmasters		
		2.2	Postmaster Complaints Handling Policy		
		2.3	Network Transaction Corrections Policy		
		2.4	Network Cash and Stock Management Policy		
		2.5	Postmaster Appeals Policy		
		2.6	Postmaster Training Policy		
		2.7	Postmaster Onboarding Policy		
09.25	3.	Whistleblowing Policy		Sally Smith	Discussion & Approval

POL00423695

POST OFFICE LIMITED

09.35	4.	Previous Meetings		Chair	
		4.1	Minutes (26 January 2021)		Approval
		4.2	Action List		Noting
		4.3	Draft Risk and Compliance Committee Minutes (16 March 2021)		Noting
09.40	5.	Risk, Compliance and Internal Audit Updates			
09.40		5.1	Risk Update	Mark Baldock	Noting
09.50		5.2	Risk Appetite Statement: Legal & Compliance	Ben Foat & Jonathan Hill	Noting & Approval
10.00		5.3	Compliance Update	Jonathan Hill	Noting
10.10		5.4	Internal Audit Update	Johann Appel	Noting
10.20	6.	Internal Audit Plan 2021/22		Johann Appel	Noting & Approval
10.30	7.	Update from Subsidiaries: verbal update Post Office Management Services (ARC)		Amanda Bowe	Noting
10.40	8.	Business Continuity Review		Jonny Lonsdale	Noting
10.50	9.	DeepDive: Payzone Governance		Andrew Goddard	Noting
11.10	10.	DeepDive: Dangerous Goods		Andy Kingham / Mark Siviter	Noting
11.25	11.	Committee Terms of Reference Review		Rebecca Whibley	Approval for onward submission to the Board
	12.	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.	Cyber Security		Tony Jowett	Noting
	2.	Procurement Governance & Compliance		Barbara Brannon	
	3.	Law & Trends		Sarah Gray & Ben Foat	
	4.	Bi-Annual Legal Risk Review (Non GLO/Starling)		Ben Foat/ Sarah Gray	
	5.	Strategic Partner Financial Stability Update		Emma Conroy/Dan Zinner	
Items for approval via Written Resolution					

POL00423695

POST OFFICE LIMITED

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/Noting		Jonathan Hill	Approval
		1.1	Summary Paper		
		1.2	Health & Safety		
		1.3	Procurement Policy		

Next ARC Meeting: Tuesday 18 May 2021 at 09.30 to 12.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ