POL ARC MEETING

21/05/2024 09:00 AM - 12:00 PM

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	21 May 2024
Time:	09:00 – 12:00 hrs
Location:	100 Wood Street, London, EC2V 7ER /Microsoft Teams. Meeting Rooms: Alder & Pine

Present:	**Invited Attendees:**
Simon Jeffreys (Chair)	Owen Woodley (Deputy Chief Executive Officer)
Andrew Darfoor (NED)	Kathryn Sherratt (Interim CFO)
Lorna Gratton (NED, UKGI)	Tim Bennett (Senior Internal Audit Manager): Item 3.4 and observing full meeting
Elliot Jacobs (NED)	Chris Brocklesby (Chief Transformation Officer): Items 3.4, 8 & 9
	Martin Roberts (Group Chief Retail Officer): Items 3.4 & 13
	Simon Oldnall (Branch Technology Director): Item 3.4
	Vishal Thanki (Data Governance Lead Contractor): Item 4
	Chris Russell (Interim Data Management Director): Items 4 & 5
Regular Attendees:	Tim McInnes (Strategy and Transformation Director): Items 4, 5 & 6
Nigel Railton (Interim Chair)	Kayleigh Dodd (Digital/Physical Records Manager): Item 5
Nick Read (Group CEO)	Jo Welch (Head of Change Risk & Assurance): Item 6
Sarah Gray (Interim Group General Counsel)	Ed Dutton (Product Portfolio Director POMS): Item 7
Andrew Paynter (Partner, PwC)	Kelly Goodwin (Programme Director):Item 8
Carol Murray (Deloitte Partner)	Neil Bennett (Chief Information Security Officer): Items 9 & 14.4
Anshu Mathur (Group Assurance Director)	Jonny Lonsdale (Business Continuity Manager): Items 10 & 14.2
Johann Appel (Director of Internal Audit)	Mark Cazaly (Head of Corporate Responsibility & Social Impact): Item 10
Jonathan Hill (Group Compliance Director)	Ross Borkett (Banking Director): Item 11
Rebecca Barker (Head of Risk)	Liam Carroll (Procurement Director): Item 12
Marie Molloy (Senior Assistant Company Secretary)	Jo Milton(Senior Operational Improvement Manager): Item 13
	Russell Hancock (Supply Chain Director); Item 13
Apologies:	Martin McKee (Head of People Services): Item 14.1
Alisdair Cameron (Group CFO)	Claire Hamilton (Speak Up and Intelligence Manger): Items 14.3 & 24
Ben Foat (Group General Counsel)	Karen McEwan (Group Chief People Officer): Item 16
Haydn Horner (Senior Manager, PwC)	Rachael Hill (Head of Talent Acquisition): Item 16
Elysia Knapp (Senior Manager, PwC)	Andy Jamieson (Head of Tax): Items 16 & 17

	Tom Lee (Group Financial Controller): Items 16, 17, 19 & 20
	Antony Ray (Specialist Senior Procurement Manager Professional and Financial Services): Item 20
	Amanda Burton (NED & Speak Up Champion): Item 24

Time		Item	Owner	Action
09.00	1.	Welcome & Conflicts of Interest	Chair	Noting
09.01	2.	Previous Meetings		
		2.1 Minutes (i) 20 March 2024	Chair	Approval
		2.2 Action List	Chair	Noting
		2.3 Risk and Compliance Committee Summary (7 May 2024)	Sarah Gray	Noting
		RISK ITEMS		
	3.	Risk, Compliance, Assurance and Internal Audit Updates		
09.10		3.1 Risk Update	Rebecca Barker	Noting/ Approval
09.20		3.2 Compliance Update	Jonathan Hill	Noting
09.30		3.3 Assurance Update • SPMP Integrated Assurance Update	Anshu Mathur	Noting/ Approval
09.40		3.4 Internal Audit Report • Investigation action assurance	Johann Appel/ Tim Bennett/ Martin Roberts/ Chris Brocklesby/ Simon Oldnall	Noting
09.50	4.	Data Governance Update	Vishal Thanki/ Chris Russell/ Tim McInnes	Noting
10.00	5.	Branch Data Plan and Controls	Kayleigh Dodd/ Chris Russell/ Tim McInnes	Noting
10.05	6.	Transformation Office Changes Update	Jo Welch/ Tim McInnes	Noting
10.15	7.	POI Board Update	Ed Dutton	Noting
10.25	8.	SPM Risk Update	Chris Brocklesby/ Kelly Goodwin	Noting

10.30	9.	Cyber Security Update - AWS Access Controls lessons learned - DLP Update	Neil Bennett/ Chris Brocklesby	Noting
10.40		*Break*		
10.45	10.	Climate risks and our approach under TCFD (Task Force on Climate-related financial disclosures)	Jonny Lonsdale/ Mark Cazaly	Noting
10.55	11.	Banking Deep Dive	Ross Borkett	Noting
11.05	12.	Procurement Governance & Compliance	Liam Carroll	Noting
11.10	13	Postmaster Policies for Approval:		
		13.1 Network Cash and Stock Management	Martin Roberts/ Jo Milton/ Russell Hancock	Approval
		13.2 Network Monitoring and Branch Assurance		
		13.3 Postmaster Complaint Handling		
	14.	Policies for Approval:		
11.15		14.1 Employee Vetting Requirements Policy	Martin McKee	Approval
		14.2 Business Continuity Management Policy	Jonny Lonsdale	
		14.3 Speak Up Policy	Claire Hamilton	
		14.4 Cyber and Information Security Policy	Neil Bennett	
11.20	15.	Post Office Insurance ARC update	Not Presented	Noting
11.20	16.	IR35 Update	Karen McEwan/ Tom Lee/ Andy Jamieson/ Rachael Hill	Noting
		AUDIT ITEMS		
11.30	17.	Tax Update and Strategy	Tom Lee/ Andy Jamieson	Approval
11.35	18.	Payment Practices Reporting Compliance	Not presented	Noting
11.35	19.	Review of External Audit (post account approval)	Tom Lee	Noting
		PWC to leave the meeting		
11.40	20.	External Auditor Procurement Exercise – Outcome and Appointment	Antony Ray/ Tom Lee	Recommendation to Board
		PwC to re-join meeting		
11.45	21.	Committee Forward Plan	CoSec	Noting/Approval

11.50	22.	Any other business	All	
11.50	23.	External Audit to meet with ARC Members		
11.55	24.	Speak Up Report	Sarah Gray/ Claire Hamilton/ Amanda Burton	Noting

Next ARC Meeting:

- 1 July 2024 at 14:00 – 17:00 Wood Street/via Microsoft Teams.

2.1

POST OFFICE LIMITED

MINUTES OF A MEETING OF THE AUDIT, RISK AND COMPLIANCE COMMITTEE OF POST OFFICE LIMITED HELD ON WEDNESDAY 20th MARCH 2024 AT 15:00 AT 100 WOOD STREET,LONDON, EC2V 7ER

Present:	**Invited Attendees:**
Simon Jeffreys **(Chair)**	Chris Brocklesby (Chief Transformation Officer): Items 3.3 & 6 **(CB)**
Andrew Darfoor (NED) **(AD)** *(joined 16.28)*	Sarah Gray (Group Legal Director): Item 4 **(SG)**
Lorna Gratton (NED, UKGI) **(LG)**	Jonny Lonsdale (Business Continuity Manager): Items 5 & 12.2 **(JL)**
Elliot Jacobs (NED) **(EJ)** *(until 16.31)*	Martin Hopcroft (Director of Health & Safety, Environment and Business Continuity): Items 5 & 12.2 **(MH)**
	Neil Bennett (Chief Information Security Officer): Item 6 **(NB)**
	Juliet Lang (Leadership and Culture Director):Item 7 **(JL)**
	Simon Recaldin (Remediation Unit Director): Item 8 **(SR)**
Regular Attendees:	Abigail Mcgeever (Strategic Partnerships Director): Item 9 **(AMc)**
Nick Read (Group Chief Executive Officer) **(NR)** *(until 16.40)*	Liam Carroll (Procurement Director): Items 10 & 12.1 **(LC)**
Owen Woodley (Deputy Chief Executive Officer) **(OW)**	Tracy Marshall (Retail Engagement Director): Item 11 **(TM)**
Kathryn Sherratt (Interim CFO) **(KS)**	Tom Lee (Group Financial Controller): Items 14 & 15 **(TL)**
Ben Foat (Group General Counsel) **(BF)**	Andy Jamieson (Head of Tax): Item 14 **(AJ)**
Andrew Paynter (Partner, PwC) **(AP)**	Rachael Hill (Head of Talent Acquisition): Item 14 **(RH)**
Haydn Horner (Senior Manager, PwC) **(HH)**	Dan Ward (Head of Financial and Technical Accounting): Item 15 **(DW)**
Elysia Knapp (Senior Manager, PwC) **(EK)**	
Carol Murray (Deloitte Partner) **(CM)**	
Anshu Mathur (Group Assurance Director) **(AM)**	
Johann Appel (Director of Internal Audit and Risk Management) **(JA)**	
Rebecca Barker (Head of Risk) **(RB)**	
Jonathan Hill (Group Compliance Director) **(JH)**	
Marie Molloy (Senior Assistant Company Secretary) **(MM)**	
Apologies:	
Alisdair Cameron (Group Chief Finance Officer) **(AC)**	

		Action
1.	**Welcome and Conflicts of Interest**	
1.1	A quorum being present, the Chair opened the meeting.	

POST OFFICE LIMITED

1.2	The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.	
2.	**Previous Meetings**	
2.1	The minutes of the Audit, Risk and Compliance Committee meetings held on 29th January 2024 were **APPROVED** and **AUTHORISED** for signature by the Chair.	
2.2	The actions were reviewed in turn. In relation to action 30, assurance over privileged access management, CM and JA discussed that the scope of the EY report on Fujitsu was still being agreed and a reassessment would be undertaken once that report was received. The ARC highlighted the importance that POL had appropriate access to perform this review. Progress against the completion of actions as shown on the action log was **NOTED**.	
2.3	BF outlined the challenging environment that POL were currently operating in and the risks these issues had caused POL, which had been reflected in the risk paper. BF also highlighted the increase in FOI's/DSAR's and their complexity. EJ was conscious of the AWS data issue and associated risks. BF advised that CB would be joining the meeting for a later item and could speak to this matter. The Risk and Compliance Committee (RCC) summary held on 12th March 2024 was **NOTED**.	
3.	**Risk, Compliance, Assurance and Internal Audit Updates**	
3.1	Risk Update RB outlined the intermediate risks outside of tolerance. Currently, POL were operating outside of tolerance for 23 out of 81 intermediate risks, a 6% increase from the January 2024 ARC update. RB highlighted ongoing pressures of the Inquiry and the impact of DSAR's/FOI requests upon a number of risks. RB reported on the scheduled deep dives undertaken on Group General Counsel, Group Commercial, Group People & Group Corporate affairs. Plans were in place to address risks at specific dates in the future, but RB advised that some may require more funding. RB discussed the risk appetite schedule, at appendix 2 of the report for which onward approval to the POL Board was being sought. The revised schedule would ensure all risks are assigned to an agreed appetite and enable improved reporting and focus on risks outside of appetite and tolerance. As part of the continuous improvement to risk management, RB was seeking ARC approval to adjust the Corporate Averse appetite scale from 1-5 to 1-6, as outlined at appendix 3 of the paper. RB explained that the change would enable risk owners to accept, as opposed to mitigate, the risk and there would also be a reduction in the amount of resource and cost to mitigate something that would still be unlikely to materialise.	

	TB outlined that, in addition, introducing this change would result in a further 41 risks being in an accept state which will also discourage risk owners forcing a lower score, which was not a risk culture POL wished to promote. RB outlined that the change would benefit the prioritisation of financial/personal resources across other risks that require action. AM discussed the data breach paper on the ARC agenda at item number 6 and considered the lack of preventative controls and potential root cause being poor behaviour to override controls. RB planned to include control effectiveness in the risk paper going forward. JA confirmed that data loss prevention was on the internal audit plan for next year. OW noted that the underlying issues were still being investigated. **ACTION**: The Chair requested that when the investigation was completed a paper to be circulated to ARC members offline. **ACTION:** The Chair outlined that, where risks are outside defined tolerance and the activity is still ongoing, there should be an explanation provided by management regarding how it was still acceptable to carry on the activity. LG discussed the risks around the FOI and DSAR requests and the relationship with the ICO. BF was mindful of POL's ability to provide the information in a timely manner and was conscious that the regulator may take a different approach with POL, if improvement was not made. AD had submitted a question via the Chair in relation to the about copper to fibre risk. RB advised that this was currently an operational risk for technology and the risk was currently outside appetite but within tolerance. RB confirmed that this operational risk was due for assessment in June 2024. In relation to risk appetite statements, the Chair clarified that some had not been reviewed since 2015. RB confirmed this was correct and she would be seeking board approval for the risk appetite statements schedule. The ARC **NOTED** the Risk Update, **APPROVED** the adjustment of the Corporate Averse appetite scale from 1-5 to 1-6 and **APPROVED** the risk appetite schedule for onward submission to POL Board.	**CB** **RB**
3.2	Group Compliance Update JH discussed the ongoing increase in both FOI requests and DSARs, mainly driven by RU & Inquiry related issues. JH acknowledged that if timeliness trends continued to dip, there was a risk that POL would be brought into special measures by the ICO. The Chair noted this was a significant reputational risk. JH was working on a plan to get back into compliance and there was a resource request submitted for the DSAR and FOI team. LG discussed the anticipation of more requests once the Inquiry restarted in April 2024. JH planned to rapidly recruit and ask for support from the rest of the business. LG also outlined her experience that senior level input was required to steer people. JH confirmed there was experienced case workers and steerco oversight. BF outlined the challenge of extracting information from the business. OW asked if the resource was in the budget and BF advised it was within the envelope submitted. The ARC **NOTED** the Group Compliance Update.	

3.3	Group Assurance Update (including SPMP Integrated Assurance) *CB entered the meeting.* AM outlined the development of a new group assurance dashboard which would cover all second line defence activity by his team. AM advised that he had expected retail to be red rated as the continuous assurance model was in the process of being implemented and AM reported upon the retail teams increased engagement with group assurance. In relation to the SPMP integrated assurance, AM reported that the integrated risk assurance universe was completed. This comprised of 505 inherent risks and circa 300 interdependencies. This would avoid duplication and facilitate adequate end to end coverage of risks when creating/executing statement of works. AM drew the committee's attention to the draft statement of works in the appendix and stated that it was his intention to present all statement of works for ARC approval in May 2024. AM was also undertaking pre-market engagement for external assurance support/SME but outlined challenges in the appointment of external assurance providers related to lack of participation (due to reputational risks perceived in the market) cost and timing issues. CB added that it was now known that DBT would like to appoint a third party to conduct assurance as well and there was a need to avoid duplication so as not to undertake the same work twice. LG considered this was not a substitute for the POL Board doing its own assurance, as the Board needed to assure itself. The ARC **NOTED** the Group Assurance update. *CB left the meeting*	
3.4	Internal Audit Report JA outlined the three audits completed during this reporting period: Stamp Stock Control rated 'Unsatisfactory', Postmaster Redress – Suspension Remuneration Review rated 'Needs Improvement' and the Cyber Maturity Assessment which was advisory and not rated. Following discussion at RCC of the IDG 2.0 audit, JA had withdrawn the report from March ARC in order to clarify the scope of the audit and this report would be submitted to May ARC. JA confirmed that completion of audit actions was progressing steadily. As of 12 March, there were 25 actions overdue, eight of which were older than 60 days. The Chair discussed the Stamp Stock Control internal audit and the timetable for fixing the issues. JA was content that management were taking action to control the gaps identified but was not sure that the timetable was sufficient. The Chair discussed the IRRELEVANT of stock and the unsatisfactory rated IA report. AP discussed that stamps were not on the POL balance sheet but noted the IRRELEVANT contract with Royal Mail Group.	

	EJ outlined that going live with auto rem was not crystallising the risk, which would be better going forward, but this would not remedy the past. JA discussed the level of uncertainty in the stock holding. EJ outlined that potentially the new system for stamps was to print them all. EJ discussed historical detriment. BF advised that the HSS scheme included stamp losses as part of the compensation scheme. EJ was not sure that Postmasters understood that HSS covers that and he undertook to review what he had been sent via correspondence and would re-raise this matter if necessary. **ACTION:** Update to be provided on the potential exposure/timing of activities in relation to Stamp stock. The ARC **NOTED** the Internal Audit Report including the progress being made with delivery of the internal audit programme and completion of audit actions. <u>Annual Internal Audit Plan</u> JA presented the proposed internal audit programme for 2024/25. LG requested that the IR 35 process was included as part of the Internal Audit plan which JA agreed to add. The ARC **APPROVED** the proposed internal audit programme for 2024/25. <u>Internal Audit CoSource Independence Report including non-audit fees</u> The ARC: • **NOTED** the statement of independence of the Internal Audit function, including Deloitte & Mazars in their capacity as the internal audit co-source providers and • **APPROVED** (ratified) the provision of other assurance work (specifically assurance over the 22/23 ARA) that resulted in the agreed 80% threshold for non-internal audit service provided by co-source providers, to be exceeded.	**Mel Park**
4.	**Legal Risk Review**	
	SG entered the meeting. SG outlined that the Solicitors Regulation Authority published its notice on Strategic Lawsuits against Public Participation ("SLAPPs") in November 2022. The notice is aimed at addressing concerns that solicitors and law firms are pursuing abusive litigation, known as SLAPPs, on behalf of their clients. A SLAPP is a misuse of the legal system, because the bringing or threatening of proceedings, in order to harass or intimidate another who could be criticising or holding a party to account for their actions may discourage scrutiny of matters in the public interest. The SRA had written to POL in relation to obligation under SLAPPs. LG asked who was written to. BF confirmed the SRA had written to him personally. SG considered that another letter was anticipated in due course and a full review of SLAPPS was being undertaken, with internal documents being updated. It was also being flagged to external firms who worked with POL.	

	SG also discussed challenges with governance, creation of the new leadership team which excluded lines of defence and issues related to delegated authority and authorised signatories which were being worked through. The ARC **NOTED** the Legal Risk Review. *SG left the meeting.*	
5.	**Safety and Physical Security Practices**	
	MH and JL entered the meeting. MH advised that whilst procedures were being reviewed and strengthened, a communication strategy was being developed to utilise appropriate channels and methods to communicate to colleagues, depending on the scenario. A threat level matrix was also being developed by the Security and H&S team which will provide clarity on controls and solutions to be implemented in the event of a threat. The Chair checked if the onboarding of the external supplier was supported by management and BF confirmed that it was and RCC had considered it appropriate and compliant with POL's duty of care. The ARC agreed with the proposed onboarding of the external supplier to assess and test security controls and to provide expert advice and guidance and training to Post Office stakeholders. The ARC **NOTED** the Safety and Physical Security Practices Report. *MH and JL left the meeting.*	
6.	**Cyber Security Update and Data Loss Prevention Suite**	
	CB and NB entered the meeting. CB introduced NB who had joined POL on 18th March. Cyber Security Update CB advised that a recent independent assessment of POL's Cyber maturity by Deloitte had confirmed that POL had successfully increased its maturity to the previous target level set in 2019. The target maturity has now therefore been increased and a Cyber programme initiated, which aims to achieve this new target by the end of 2026. CB noted that this target could be achieved faster with additional funding as the original funding request for FY25 has been reduced from IRRELEVANT The total Cyber investment required was expected to be circa IRRELEVANT Phase 1 was now estimated to be IRRELEVANT which CB advised was in line with available funding. CB highlighted the threat landscape, with threat actors increased sophistication and POL's high profile. The ARC discussed the IRRELEVANT target maturity and whether this was correct. CB confirmed that the new target would be confirmed by NB.	

2.1

POST OFFICE LIMITED

	Data Loss Prevention (DLP) Suite CB discussed the lack of preventive controls, and therefore IRRELEVANT IRRELEVANT IRRELEVANT Specifically, the Cyber team IRRELEVANT IRRELEVANT CB mentioned that the business had IRRELEVANT IRRELEVANT CB confirmed that the March RCC had supported the short-term recommendations to introduce more preventive controls and bring POL into risk tolerance. It was acknowledged that this would impact the ease of access to systems and prevent access to some personal applications but would significantly reduce the risk of data loss. **ACTION:** DLP update to be provided to May ARC. EJ asked about the AWS data breach. CB confirmed that the control failures were being investigated. OW outlined there were incorrect audit settings on the database so there was no evidence that the data had not been seen. LG asked about the reaction of those stakeholders informed. CB confirmed they had been advised via the commercial team who looked after the commercial relationship. OW noted that it was poor timing in relation to Banking Framework 4 negotiations and generally there had been understanding, but consciousness of the impact on security of the NBIT release. *AD joined the meeting at 16.28.* From early root cause analysis, CB outlined that people had been assigned the wrong access. LG asked about CB's sense about wider controls. CB believed that there was not widespread control indifference generally and an access control roles based process was in place. The ARC **NOTED** the Cyber Security Update and Data Loss Prevention Suite *CB and NB left the meeting.*	**NB**
7.	**Mandatory Training: Status, changes and enhancements**	
	JL entered the meeting. *EJ left the meeting at 16.31.* The Chair asked JL to interpret how good or otherwise the performance was from the bar chart at the paper appendix. JL advised that reports had been re-run and all modules now had a greater than 95% completion rate and so the compliance target was met. JL reported that 88 individuals had one or more compliance modules that were incomplete. The Chair asked if this would be taken into account on their appraisal. JL advised they had until 31 March 2024 to complete the modules or they would be ineligible for any bonus opportunity. **ACTION:** An update on compliance achieved at 31 March 2024 to be provided to ARC.	**JL**

	AD was interested in POI compliance adhere as a regulated entity. **ACTION:** JL to ascertain from POI its compliance adherence. The ARC **NOTED** the Mandatory Training: Status, changes and enhancements report. *JL left the meeting.*	**JL**
8.	**Remediation Unit (RU) Risk & Assurance Update**	
	SR entered the meeting. SR highlighted the RU Intermediate Risks, set out at appendix 1 of the paper, and the worsening risk profile across the RU. SR discussed the impact of recent government announcements. In addition, the number of late applications to HSS, which was likely to materially increase, may not be capable of being fulfilled by HSF and the current panel members. SR further outlined challenges in the RU people space. NR confirmed that POL were waiting on clarity on what DBT wanted to do. LG confirmed that a solution was being worked on, but this was not straightforward. SR outlined that the outcome of the Internal Audit (IA) across HSS had provided helpful improvements. JA confirmed that three of the five key actions raised by IA had now been closed, with target dates for closure of the other two set for the end of the year. The ARC **NOTED** the Remediation Unit Risk & Assurance Update. *SR left the meeting.*	
9.	**Strategic Partner Risk & Failure Monitoring Deep Dive**	
	AMc entered the meeting. AMG presented the Strategic Partner Risk & Failure Monitoring Deep Dive. The ARC **NOTED** the Strategic Partner Risk & Failure Monitoring Deep Dive. *AMc left the meeting.* *NR left the meeting 16.40.*	
10.	**Procurement Risk & Compliance Report**	
	LC entered the meeting. LC presented the Procurement Risk & Compliance Report. The ARC **NOTED** the Procurement Risk & Compliance Report *LC left the meeting.*	
11.	**Postmaster Policies for Approval**	
	TM entered the meeting. TM presented the following Postmaster policies for ARC approval: • Network Transaction Corrections	

	• Postmaster Onboarding • Postmaster Training Policies (Annual Review) TM outlined that specific feedback from the internal policy assurance reviews completed by the Group Assurance (GA) team had been incorporated, where applicable, into these policies. In addition, the assurance review had highlighted a number of actions, and these are being worked through as quickly as possible by the retail team. TM confirmed that a review of risks and controls within all of the suite of Postmaster policies would be completed by the end of July 2024. The GA team were supportive of these three policies being submitted for approval in the meantime, given the importance of ensuring annual reviews were undertaken. LG asked about feedback from those impacted by the policies and what it felt like to be on the receiving end of the policies. BF confirmed there was stakeholder engagement and TM confirmed that the NFSP were involved and signed off the policies. AD enquired about how the success of the policies/any improvement was measured, from the lens of the end user. TM confirmed there were KPI's monitoring this such as the training experience and support. TM was working with GA to develop this dashboard further. AM agreed KPI's/KRI's needed to be looked at end to end from a Postmaster lens. **ACTION:** Presentation to ARC and Board of the dashboard, once it has been developed. *TM left the meeting.*	**TM**
12.	**Policies for Approval**	
12.1	*LC entered the meeting.* Procurement Policy LC advised that the team were awaiting enactment of secondary legislation and therefore the policy was likely to be further amended in the future, to take this secondary legislation into account. The ARC **APPROVED** the Procurement Policy. *LC left the meeting.*	
12.2	MH and JL entered the meeting. Health and Safety Policy MH presented the Health and Safety Policy. The ARC **APPROVED** the Health and Safety Policy. MH and JL left the meeting.	
13.	**Post Office Insurance ARC update**	
	This item was not presented.	

	The ARC **NOTED** the Post Office Insurance ARC update.	
14.	**IR35 Update & Decisions & People Risks**	
	TL, AJ and RH entered the meeting. TL advised that management were seeking ARC approval to pursue option 2, as outlined in the paper. This would mean that POL could continue to debate the position with HMRC, seek to review the contractor population and negotiate a settlement, which should be considerably lower than the worst-case scenario, albeit noting the precedent risk highlighted within the Corporation Tax funding offer paper to Board of 28 Feb 24. TL outlined that this option would still be likely to lead to a significant number of IRRELEVANT assuming HMRC's stance is followed. Contemporaneously, management would seek to amend the policy and process for engaging and renewing contractors, de-risking the position by IRRELEVANT TL added that HMRC had IRRELEVANT and so could consider the IRRELEVANT There was also a risk to programmes such as RU and SPMP in trying to IRRELEVANT and the potential loss of resource. IRRELEVANT in the assessments was discussed. TL outlined that IRRELEVANT had been assisting with the HMRC correspondence . The Chair asked about internal assurance and TL confirmed that the legal, people and tax team had been involved. TL advised that HMRC had not shared a view until December 2023. The Chair had the sense that POL thought that it had a defensible position. LG noted the position was that another organisation has lost on. TL was aware that DWP had lost a case but did not know this was in relation to IRRELEVANT, as this was not publicly available information. AJ added that on 1 April 2017 IRRELEVANT were engaged to advise POL how to set the scheme up. LG asked that when HMRC raised the IRRELEVANT why POL did not change its policy or get legal advice on the strength of its position. TL outlined that POL did not get advice on the strength of position, the advice was on the policies, approach and HMRC correspondence. LG considered that management decisions may have resulted in higher liability than may otherwise have been the case. TL advised that management kept the ARC informed. **ACTION:** The Chair requested that management put together a chronology of events and rationale so what had happened could be understood in preparation for discussion with DBT and there was urgent action on the contractor population to de-risk the position. In relation to the assessment of the current contractor population, KS advised that the people team were leading on this. RH outlined that of the total 341 contractors, around 150 contractors are supplied through an IRRELEVANT IRRELEVANT	 **TL/RH**

	The ARC was supportive of management pursuing option 2; to debate the position with HMRC, seek to review the contractor population and negotiate a settlement above. *AJ and RH left the meeting.*	
15.	**FY23/24 ARA plan and Revaluation Policy Review**	
	DW entered the meeting. TL enquired if the Deloitte assurance activities undertaken in the prior year should be repeated for FY23/24. The ARC confirmed that they should be as it had been a useful exercise. JA discussed the security headroom with the first breach projected falling within the going concern period. TL confirmed he was monitoring the position and the requirement for waivers and extensions of facilities was being considered and worked on as required. TL advised that overall, the payout levels across the Remediation Matters schemes were expected to increase significantly when compared with the estimated levels included in the FY22/23 provisions. The net effect was therefore likely to be an increased provisioning level driven by late applicants to the HSS scheme, policy changes to HSS to increase the minimal payment level to £75k, the mass exoneration of previous convictions and the recognition of a provision for the Post Office Process Review, which was disclosed as a Post Balance Sheet Event in the FY22/23 ARA. TL outlined that the OC provision may decrease as the mass exoneration may be fully settled directly by government. TL outlined the key risk for the ARA was that the revised estimates for both the IRRELEVANT IRRELEVANT Wrongful trading was discussed with LG advising there was clarity that the department were fully funding the costs of RM. In relation to IRRELEVANT a provision will likely be recognised in the ARA in respect of this and appropriate disclosures, outlining the change, the rationale and the funding commitment will be included. TL advised that most recent estimates indicated that historical liabilities will be significantly reduced vs the previous estimates, due to the ability to utilise built up allowances and losses, albeit noting this exposes POL to the risk of future IRRELEVANT arising as losses will be greatly diminished. LG outlined the impact this underspend had on the DBT and Treasury and was keen to ensure this was done differently to not impact their budgets in this manner. TL was conscious that matters were still with IRRELEVANT and so the numbers could potentially change again, whilst also noting DBT had requested a worst-case estimate, which was provided. In relation to CGU Impairment, TL advised that the latest forecasts indicated a slight strengthening of trading profit when compared with that used for the FY22/23 analysis. However, trading losses are still forecasted presently, and management remain cautious as the budget process for FY25/26 is still underway and maintaining an impairment unless sufficient confidence in longer term trading is established, would be sensible. Detailed modelling will be performed as part of the yearend ARA process.	

TL discussed a key variable driving the timeline for signing of the FY23/24 ARA was the going concern position, with ARC and PwC's views on what constitutes sufficient evidence and assurances to support a going concern assumption being pivotal. Additionally, the timing of a General Election and what that means for BAU funding, being NSP and Investment funding, should be considered. In addition, the Fujitsu contract renewal was a key determinant of the going concern position.

The ARC determined that the working assumption should be that a summer signing timeline should be aimed for with dates provided/mapped for when decisions would need to be made to achieve this, albeit with close monitoring of forecasts, funding/support requirements and other matters, such that signing could be pushed back if required.

In relation to content, presentation and positioning, the ARC agreed with managements recommendation to keeping any changes to a minimum until such time as there is enough bandwidth in the organisation to deal with these.

Revaluation Policy

TL outlined that the implementation of a revaluation policy would not be in line with expectations of a business of POL's nature and would also introduce greater cost and complexity into POL accounting processes and the associated external audit. A move to a revaluation method would constitute a change in accounting policy, rather than accounting estimate, adding further complexity Following discussion, the ARC agreed that POL continue with the cost model.

The ARC **NOTED** a number of expected accounting and disclosure updates to be included in the FY23/24 ARA, including some expected PBSE items.

DW left the meeting.

16. PwC Final Audit Plan

AP presented the PwC final audit plan and highlighted that the tax risk had increased. HH outlined the ARC responsibilities in relation to fraud risk referenced at appendix 3 of the report.

The ARC **APPROVED** the PwC Final Audit plan and the following non-audit services in relation to the FY24 year end:

- Royal Mail AUP
- DVLA AUP
- DBT AUP
- BoE Note Circulation Scheme NAAE
- Branch Network KPI NAAE

17. Committee Forward Plan

The ARC **NOTED** the Committee Forward Plan.

18. Any other business

There was no further business raised.

19.	**External Audit to meet with ARC Members**	
	AP, HH and EK met with the Chair, LG and AD. MM was present to capture notes of the meeting. CM was in attendance.	
	There being no further business, the meeting was closed at 18.11	

....
Chair

....
Date

Post Office Limited Audit, Risk & Compliance Committee
OPEN ACTIONS

Number	Meeting Date	Minute Reference	Action	Action Owner	Due Date	Comment
1	3/28/2023	4	**ACTION:** A plan to be presented to ARC regarding branch data.	Kayleigh Dodd/ Chris Russell	May-24	08/05/2024: Item on the agenda for May ARC. **Action proposed for closure.** 01/03/2024: This item will be further addressed at May 2024 ARC due to personnel absence for March 2024. 22/01/2024: Chris Russell to present an interim verbal update to January 2024 ARC at item 8 on the agenda. 06/11/2023: Action deferred to January 2024 as our strategy for branch data is being revisited and we do not have definitive options or answers for the ARC at this time. 01/09/2023: Kayleigh Dodd is intending to present to IADG regarding physical data in October with an updated prove plan and will revert after this to November ARC. 16/06/2023: This will be presented to September ARC having been reviewed by GE.
2	9/25/2023	3.1	**ACTION:** Interim Data Management Director to present a remediation plan to ARC in November 2023.	Chris Russell	May-24	08/05/2024: Data Management will be presenting to May ARC a paper that looks at the following issues. 1.Risk – Current Risk level for Data Management and short, medium and long term activities to bring it within POLs Risk Appetite 2.Planned Activities – Work being led by DM to bring POL to a minimum of Level 4 maturity for all POL critical data sets. This will include proposed Pilot areas to be covered. 3.Timelines for the various activities and stages 4.Resourcing and Structure. 5.Next Steps. **Action proposed for closure.** 01/03/2024: Deferred to May 2024 due to personnel absence. 22/02/2024: Chris Russell to present an interim verbal update to January 2024 ARC. A paper will be presented to March 2024 ARC.
3	11/12/2023-ARA Sub-Committee	2.2	**ACTION**: KS to work with Martin Roberts (Group Chief Retail Officer) and Melanie Park (Central Operations Director) on the memo previously prepared in respect of related party transactions.	Kathryn Sherratt	May-24	08/05/2024: Kathryn advised that this action could be closed. **Action proposed for closure.** 01/03/2024: This is in progress
4	1/29/2024	3.1	**ACTION:** RB would revert to ARC with further information regarding the retail operational risk and the amendment to include the principle of fairness.	Rebecca Barker	May-24	10/05/2024: The risk was updated in December to reflect fairness within the risk name and description ensuring that it is visible that fairness is addressed across the remediations. Position included in the retail deep dive: Remediation efforts to mitigate this risk are advancing, and retail remain steadfast in ensuring that our actions across all remediations result in fair and consistent treatment for our postmasters. This commitment aligns with our strategic objective of rebuilding trust. The size and sustainability of improvements maybe limited without additional resource, future funding has been requested through the SPM project in order to facilitate a healthy network and support a successful NBIT implementation. **Action proposed for closure.**
5	1/29/2024	3.3	EJ enquired about fake currency notes charged to Postmasters and the potential of detriment on that. **ACTION:** AM agreed to follow up the fake currency issue and report back to ARC.	Anshu Mathur	Jul-24	08/05/2024: Anshu is still progressing this action.
6	1/29/2024	5	**ACTION:** CB/KG to revert back to ARC with a formally documented list of SPMP risk and the parameters in which they will operate for releases, especially with a PM lens.	Chris Brocklesby/ Kelly Goodwin	Jul-24	13/05/2024: Interim update provided to May 2024 ARC. 11/03/2024: This will be presented to May 2024 ARC.
7	1/29/2024	6	**ACTION:** The chair requested that for the next iteration of the report, the residual risk assessed after mitigation was provided.	Chris Brocklesby	Jul-24	
8	1/29/2024	8	AD asked about the split between physical and digital data. CH advised that historical data was very much physical and more recent and ongoing data was digital but she was not aware of percentages. **ACTION**: AD requested clarification of the stage the business started at and where it had got to in its migration to digitisation and the timeline anticipated for completion.	Kayleigh Dodd	May-24	25/04/2024: The vast majority of Post Office records are now created and stored in a digital format, however there remains over 80,000 boxes of physical records in storage. Many of these no longer hold any business value and are overdue disposal, but they continue to be retained under the terms of the document preservation holds which are currently in place across the business. A simple analysis suggests that over 27,000 (34%) of the boxes were submitted to storage over 10 years ago. This increases to over 52,000 (65%) which were submitted over 7 years ago. Most of these boxes are highly unlikely to be reviewed again and will be fit for immediate disposal once the preservation holds are lifted. The remaining boxes are expected to be mainly branch accounting records which are also unlikely to be reviewed again and so there is limited value in digitising. When the document preservation holds are lifted a disposal process will commence and significantly reduce the number of physical records held in storage. Whilst the Data Management Team consistently review the options and benefits of digitising legacy physical records, or a subset of records, in the current environment there appears to be little value in migrating all physical records to digital. The Data Management Team are in the process of supporting the business to identify Data Owners for any physical records, with an aim of working together to minimise the creation of physical records in the future. **Action proposed for closure.**

9	1/29/2024	8	EJ discussed disposal/shredding of branch data that did not need to be held and liability/responsibility for this. Fly tipping of Moneygram forms was used as an example and EJ highlighted the cost of proper disposal and the reputational risk. **ACTION:** Kayleigh Dodd to address in her report to ARC in May 2024	Kayleigh Dodd	May-24	25/04/2024: please refer to response to action no 8. **Action proposed for closure.**
10	1/29/2024	12	JL advised that the Cyber Security Team were planning on conducting a robust Ransomware attack test but there was currently no date for when the ransomware test was scheduled. **ACTION:** ARC to be notified of the cyber testing date.	Neil Bennett	Jul-24	13/05/2024: The Purple Team exercise concluded and learnings are being incorporate in to the Security Operations Centre ways of working. Broader ransomware exercising is a key stream of the Cyber Security Maturity Programme, with the business case currently being in the approvals process 12/03/2023: The Cyber team (Ross Welton) has confirmed whilst there are no ransomware specific tests scheduled, there are some Red teams (Attacking Team) etc due to run and they are also currently running a Purple team (response teaming) with nettitude on NBIT. The Ransomware planning now forms part of the Cyber Security Maturity Programme
11	1/29/2024	14	**ACTION:** In relation to the Committee Evaluation the Chair requested that the templates were reviewed in line with current evolution of the Committee.	CoSec	Jul-24	13/05/2024: a review of templates is being undertaken.
12	3/20/2024	3.1	**ACTION**: The Chair requested that when the investigation was completed a paper to be circulated to ARC members offline.	Chris Brocklesby	Jul-24	
13	3/20/2024	3.1	ACTION: The Chair outlined that, where risks are outside defined tolerance and the activity is still ongoing, there should be an explanation provided by management regarding how it was still acceptable to carry on the activity.	Rebecca Barker	Jul-24	17/05/2023: Plan to commence for July ARC.
14	3/20/2024	3.4	**ACTION:** Update to be provided on the potential exposure/timing of activities in relation to Stamp stock	Mel Park	Jul-24	
15	3/20/2024	6	**ACTION:** DLP update to be provided to May ARC.	Neil Bennett	May-24	17/05/2024: Update included in the paper.
16	3/20/2024	7	**ACTION:** An update on compliance achieved at 31 March 2024 to be provided to ARC.	Juliet Lang	May-24	17/05/2024: There was 98.7% completion across all modules. The internal target for completion (95%) across all modules which was met.
17	3/20/2024	7	AD was interested in POI compliance adhere as a regulated entity. **ACTION:** JL to ascertain from POI its compliance adherence.	Juliet Lang	May-24	28/03/2024: JL received the following response from POI: Post Office Insurance colleagues are included in the mandatory training compliance data modules that were presented to ARC. They currently complete Anti-Money Laundering, Information security, Data Protection and Anti-Bribery and Corruption. In addition, at 1-1s and performance reviews POI colleagues also concentrate on other more specific needs. Perhaps the best example over the last year is the plain English training that they conducted as part of their ongoing commitment to Consumer Duty Compliance POIs outsourced customer service teams (now Webhelp) have their own detailed training requirements which they sign off as part of their control processes. POI review compliance and calibrate call monitoring regularly. Since 2017 /18 POI designed the system in such a way that the training records are linked to systems access and training for front line colleagues. This means that unless insurance specific, and some other training, has been complete then individual staff members cannot sell our insurance products. This is a very effective control and ensures that 100% of staff who sell our product are trained to do so. **Action proposed for closure.**
18	3/20/2024	11	**ACTION:** Presentation to ARC and Board of the dashboard, once it has been developed.	Tracy Marshall	Jul-24	
19	3/20/2024	14	**ACTION:** The Chair requested that management put together a chronology of events and rationale so what had happened could be understood in preparation for discussion with DBT and there was urgent action on the contractor population to de-risk the position.	Tom Lee/Racheal Hill	May-24	15/05/2024: Item addressed at May ARC agenda item 16. **Action proposed for closure.**

2.3

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE

Title:	Summary of key discussion and outcomes	**Meeting Date:**	21 May 2024
Author:	Sarah I Gray, Interim Group General Counsel	**Sponsor:**	N/a

Input Sought: Noting

The Committee is asked to:

- **Note** key discussions and actions arising from the Risk & Compliance Committee (RCC) on 7 May 2024.
- Please note this is not intended to override the formal RCC minutes, and that the full agenda can be found in **Appendix 1**.

1.0 Summary of RCC – 7 May 2024

1.1 RCC Structure and Approach

The Interim Chair reminded the RCC members that the RCC structure, content, coverage and governance was still under review, and that the Group General Counsel on his return in June 2024, should be reaching out to members to commence the assessment of how the RCC could be improved.

1.2 RCC Actions

The RCC debated whether the risk definition to capture 'Treating Postmaster's (PM) fairly' was robust and appropriate. The Committee was made aware that the definition had been updated by both Group Risk and Retail in December 2023. The RCC requested that the definition be circulated outside of the meeting to relevant members to ensure RCC was comfortable with the definition and its coverage.

1.3 Risk Update, including Strategic Risk Management Review

See 1.2.

It was observed that certain key risks needed to be captured to ensure the risk overview to ARC reflected the environment in which POL was currently operating under, for e.g. SPMP Programme Deliverability, People Wellness etc. The RCC requested that the paper should be structured to reflect the feedback from the ARC Chair in March 2024 primarily – out of tolerance (OOT) risk, period since when OOT, whether compensating control exists, can POL do more, or do these require formal risk acceptance.

RCC queried the divergence between the Retail Risk Deep dive showing 23 of 29 risks mapped to controls and rated as effective, against the Assurance update which was predominantly red. The Head of Risk, Retail and Assurance were to ensure alignment prior to ARC.

It was agreed that Risk team would be part of the 3-4 year business plan review to ensure an appropriate assessment could be made on funding requirements and their impacts on associated risks profiles.

To allow for appropriate input from the Interim Chair, the RCC decided that the Strategic Risk Management Review should be deferred to the next RCC/ARC.

1.4 Compliance Update

RCC was made aware that the ICO intended to issue a formal Practice Recommendation (PR) to POL following concerns as to PO's response times to FOIs. The ICO had asked POL to respond by 17 May to a number of questions; the responses to which will shape the PR. The RCC was made aware that should there be noncompliance with PR and/ or lack of engagement with the ICO, that this could result in a possible enforcement notice.

FOIA request and resourcing levels in the team were discussed, and it was recognised that this continues to be challenging, with impacts on people's wellbeing becoming much more overt. Whilst funding was available to resource the FOIA team to deal with volumes of request, recruitment had a time lag, compounded by upskilling of new recruits.

The Compliance Director assured the Committee that the absence of a permanent MLRO was not having a detrimental impact, and that interviews had begun to find a suitable replacement. HMRC has been informed, and the Compliance team have in place 2 'Recognised Officers' to ensure continuity.

1.5 Group Assurance Update

RCC noted the continuing unsatisfactory assurance outcomes for Retail, for both Continuous Assurance and Overdue Management Actions. The RCC was informed that whilst the overall status was red, the engagement with the Retail Team, including a change in their approach to reviewing artefacts/evidence for controls, should in the medium term begin to show improvements. That said it was challenging to determine when this would be. In addition, the significant increase in overdue actions related to PM Policy Reviews which were due end March, and now reforecast to the end of June.

The RCC discussed whether Group Assurance resources should be diverted to support SPMP Assurance, and RCC agreed that this should not be allowed given the criticality to assess the BAU control environment.

The Group Assurance Director (GAD) provided an overview of the SPMP Assurance Statement of Works (SoW) and how coverage was assured across the SPMP Pillars. GAD highlighted that progress on delivering the reviews was lacking pace, and that a risk existed that POL may not have the right composition and experience within the internal POL Assurance teams to deliver. This is compounded by the process to procure external assurance support. The SPMP programme recognise the importance to deliver the Assurance plan and have approved the recruitment of 2 additional Assurance resources. The RCC requested the GAD to keep them informed if this risk materialised.

1.6 SPMP Update - Risk Profile

RCC received a verbal update from the SPMP Programme Director, highlighting the significant amount of progress that had taken place over the last three months to understand their risk profile e.g. creation of the assurance universe, external reviews, draft release strategy. The Committee noted that whilst the direction of travel was good, a formalised view on risk vs release strategy was still being developed and it was unlikely to be ready for the May ARC. An externally facilitated risk workshop was planned. The RCC agreed that a paper should be submitted to ARC outlining the steps taken to date, with a clear articulation of what is still needed and by when in order to provide a formalised risk assessment vs release strategy.

1.7 Internal Audit Update

RCC discussed the Horizon Privileged Access Management update and enquired why the report remained in draft and contained no opinion. Internal Audit will be updating their paper ahead of ARC to provide an overlay.

1.8 Data Governance Update

The interim Data Management Director provided his vision to enhancing the data maturity profile of POL to IRRELEVANT by June 2024, and to IRRELEVANT RCC challenged whether this was ambitious enough and whether this fell short of the feedback from ARC received last year i.e. to speed up maturity with more stretching timelines and targets. The Director will revisit the paper to make clearer how maturity will be achieved and by when.

1.9 IRRELEVANT

1.10 Finance Update – IR35/ Tax Update/Strategy

Finance presented their detailed update on the chronology of events and advise / input received in relation to IR35, along with a detailed Tax strategy paper which the RCC fully endorsed. The RCC acknowledged that a risk existed in relation to tax exposure and funding regarding IR35, and all roles will need to be assessed based on their enduring nature and criticality, which is currently being worked through.

1.11 PM Policies / Policies for Approval

All three PM policies (Network Cash and Stock Management, Network Monitoring and Branch Assurance and Postmaster Complaint Handling) and four other Group polices (Employee Vetting Requirements Policy, Business Continuity Management Policy, Speak Up Policy, Cyber and Information Security) were approved for onward submission for ARC approval in May 2024.

Appendix 1 – Risk and Compliance Committee Agenda – 7 May 2024

Meeting:	Risk and Compliance Committee
Date:	Tuesday 7th May 2024.
Time:	09:45 – 13:00
Location:	Wood Street: Birch/via Microsoft Teams

Present:	**Attendees:**
Sarah Gray (Chair) Interim Group General Counsel	Johann Appel (Director of Internal Audit)
Max Jacobi (Finance Director – Commercial)	Rebecca Barker (Head of Risk)
Tracy Marshall (Retail Engagement Director)	Christian Spelzini (Interim Group Legal Director)
Nicola Marriott (HR Director) on behalf of Karen McEwan	Jonathan Hill (Group Compliance Director)
Kathryn Sherratt (Interim Chief Finance Officer)	Anshu Mathur (Group Assurance Director)
	Tom Lee (Group Financial Controller)
	Marie Molloy (Senior Assistant Company Secretary)
	Ross Borkett (Banking Director): Item 4
	Vishal Thanki (Data Governance Lead Contractor): Item 5
Apologies	Julian Hilditch (Inquiry Data & Disclosure Lead Contractor): Item 5
Alisdair Cameron (Group Chief Finance Officer) - TBC	Chris Russell (Interim Data Management Director): Items 5 & 6
Karen McEwan (Group Chief People Officer)	Tim McInnes (Strategy and Transformation Director): Items 5, 6 & 7
Owen Woodley (Deputy Chief Executive Officer)	Kayleigh Dodd (Digital/Physical Records Manager): Item 6
Ben Foat (Group General Counsel)	Jo Welch (Head of Change Risk & Assurance): Item 7
Chris Brocklesby (Chief Transformation Officer)	Kelly Goodwin (Programme Director NBIT): Item 8
	Neil Bennett (Chief Information Security Officer): Items 9 & 17.4
	Liam Carroll (Procurement Director): Item 10
	Tim Perkins (Programme Director): Item 11
	Jazz Chand (Head of Cash Production, Planning and Optimisation): Item 14
	Martin Hopcroft (Director of Health & Safety, Environment and Business Continuity): Items 16 & 17.2
	Jonny Lonsdale (Business Continuity Manager): Items 16 & 17.2
	Mark Cazaly (Head of Corporate Responsibility & Social Impact): Item 16
	Martin McKee (Head of People Services): Item 17.1
	Claire Hamilton (Speak Up and Intelligence Manger): Item 17.3
	John Bartlett (Director of Assurance & Complex Investigations): Item 17.3

2.3

Time		Item	Owner	Action
09:45- 09:46	1.	Welcome & Conflicts of Interest	Chair	Noting
09:46- 09:50	2.	Previous Meetings		
		2.1 Minutes (12 March 2024)	Chair	Approval
		2.2 Action List		
	3.	Risk, Compliance, Assurance and Internal Audit Update		
09:50- 10:00		3.1 Risk Update • Strategic Risk Management Review	Rebecca Barker	Approval (onward submission to ARC)
10:00- 10:10		3.2 Compliance Update	Jonathan Hill	Approval (onward submission to ARC)
10:10- 10:20		3.3 Assurance Update • SPMP Integrated Assurance Update	Anshu Mathur	Approval (onward submission to ARC)
10:20- 10:30		3.4 Internal Audit Report	Johann Appel	Approval (onward submission to ARC)
10:30- 10:40	4.	Banking Deep Dive	Ross Borkett	Approval (onward submission to ARC)
10:40- 10:50	5.	Data Governance update • POL Inquiry e-Data Assurance Review (Verbal Update)	Vishal Thanki/ Chris Russell/ Julian Hilditch/ Tim McInnes	Approval (onward submission to ARC)
10:50- 11:00	6.	Branch Data Plan and Controls	Kayleigh Dodd/ Chris Russell/ Tim McInnes	Approval (onward submission to ARC)
11:00- 11:10	7.	Transformation Office Changes Update	Jo Welch/ Tim McInnes	Approval (onward submission to ARC)
11.10- 11:15	8.	SPMP Risk Update (Verbal Update)	Kelly Goodwin	Approval (onward submission to ARC and Board)
11:15- 11:25	9.	Cyber Security Update • AWS Access Controls lessons learned • DLP Update	Neil Bennett	Approval (onward submission to ARC)
11:25- 11:30	10.	Procurement Governance & Compliance	Liam Carroll	Approval (onward submission to ARC)

11:30- 11:35		*Break*		
11:35- 11:45	11.	IR35 Update	Tom Lee/ Tim Perkins	Approval (onward submission to ARC)
11:45- 11:55	12.	Tax Update and Strategy	Tom Lee	Approval (onward submission to ARC)
11:55- 12:00	13.	Payment Practices Reporting Compliance	Tom Lee	Approval (onward submission to ARC)
	14.	Postmaster Policies for Approval		
12:00- 12:10		14.1 Network Cash and Stock Management	Tracy Marshall/ Jazz Chand	Approval (onward submission to ARC)
		14.2 Network Monitoring and Branch Assurance		
		14.3 Postmaster Complaint Handling		
12:10- 12:20	15.	SRA's SLAPP Notice	Christian Spelzini	Noting
12:20- 12:40	16.	Climate risks and our approach under TCFD (Task Force on Climate-related financial disclosures)	Martin Hopcroft/ Jonny Lonsdale/ Mark Cazaly	Approval (onward submission to ARC)
	17.	Policies for Approval:		
12:40- 12:50		17.1 Employee Vetting Requirements Policy	Martin McKee	Approval (onward submission to ARC)
		17.2 Business Continuity Management Policy	Martin Hopcroft/ Jonny Lonsdale	
		17.3 Speak Up Policy	Claire Hamilton/ John Bartlett	
		17.4 Cyber and Information Security Policy	Neil Bennett	
12:50- 12:55	18.	Audit, Risk & Compliance Committee pre-meeting review	Chair	Noting
		18.1 ARC Agenda – 21 May 2024		
		18.2 Forward Plan (including RCC only items)		
12:55	19.	Any other business	All	Noting
Next RCC Meeting: Thursday 13 June 2024 from 10:30 to 13:30 at Wood Street/via Microsoft Teams				

POST OFFICE

POST OFFICE LIMITED
AUDIT RISK & COMPLIANCE COMMITTEE REPORT

3.1

Title:	Risk Update	**Meeting Date:**	21st May 2024
Author:	Rebecca Barker (Head of Risk)	**Sponsor:**	Sarah Gray (Interim Group General Counsel)

Input Sought: Approve

The committee is requested to:

i. Note our key risk position and the target dates to bring into tolerance
ii. Approve: the suggested appetite & tolerance levels for Strategy & Environment risk appetite statements

Executive Summary

This report is focussed on the intermediate risks outside of tolerance. Currently, we are operating outside of tolerance for 23 out of 74 intermediate risks.

The report highlights risks with a RAG rating of red or amber, which denotes the status of the remediation plan, and if it is on plan to remediate the risk within the agreed target date.

Change spend review has been agreed for 2024/25 which supports remediation activities for several intermediate risks. This review has highlighted risks which may not have sufficient funds to ensure remediation within proposed target dates.

We conclude: Risk appetite and tolerance levels play a crucial role in informed decision-making. They provide the necessary confidence in our response to risks and ensure transparency regarding the intermediate risks we face and how we manage them.

However, it is important to acknowledge that our control framework maturity is an ongoing journey. At this stage, we cannot definitively state that the controls managed within our governance risk tool effectively reduce risk. Nevertheless, risk owners are diligently working on detailed remediation plans with specific target dates to bring risks within acceptable tolerance levels.

The central risk team remains committed to collaborating with risk owners, ensuring timely delivery, and addressing any concerns. Our remediation RAG rating (appendix 1) continues to highlight areas of concern to the committee.

Throughout our discussions with the first line, a consistent theme emerges—the well-being of our colleagues. The impact of the inquiry, negative social media, and the capacity of colleagues to perform day-to-day activities are all critical factors on the management of risk which we must consider.

Top risks outside of tolerance

Appendix 1 outlines **all** intermediate risks that fall outside of tolerance levels, along with their target dates and RAG ratings. The risks mentioned below are flagged for awareness because their current remediation status is either Amber or Red. This indicates concerns that ongoing activities may not sufficiently reduce the risk by the agreed-upon target date.

1. Technology

- The risk of the **End of Horizon support Agreement** remains outside tolerance. Formal discussions commenced with Fujitsu on extension beyond March '25 for a period up to

3.1

5 years. Signing of the contract is planned for October '24. Remediation is unlikely to complete by March 2025.

- The risk of **moving the network from copper to fibre** has increased and is outside of tolerance. Failed install rates remain high, due largely to a recognised gap in Postmaster communications across the programme portfolio, supplier communication issues, and site-specific challenges due to prior site assessments not being funded. The project is reporting the overall status of delivery as amber. A recent Internal Audit determined that the project is a "Significant Delivery Risk". Activity is underway by the programme and business sponsor to address these issues to ensure end date of December 2025 is met.
- **Branches unable to process Paystation transactions** currently outside of tolerance. There is a Second Device project which will replace Paystations with the Second Device supporting a bespoke software solution also providing legacy pre-paid bill payment products. Funding has been agreed until June 2024 to purchase hardware and continued to development, the project delivery status is currently rated red. Remediation is unlikely to complete by March 2025.

2. **Security**

- **Inability to prevent Cyber or ransomware attacks & Inability to recover from Cyber attacks**. Both risks are outside of tolerance. Funding of IRRELEVANT has been agreed for 2024/25. IRRELEVANT

IRRELEVANT

3. **Legal**

- Risk of **Non-compliance with Statutory & Regulatory Requirements** risk remains outside of tolerance. The number of FOI cases related to the Remediation Unit remains high. The ICO are aware of the unique position of Post Office and have been provided with a plan to bring this back into compliance. Eight new roles have been approved (1 already in place). Recruitment of the remainder is in progress. These are full time contracts for 12 months to help & support achieve regulatory compliance. Currently the remediation plan remains off-track.
- **Inability to either retain or attract Legal talent** risk remains outside of tolerance. The risk is impacted by the increasing media attention and SRA (Solicitors Regulation Authority) investigations. A decision on future funding is required, until such time the remediation plan remains off-track.

4. **Financial**

- **Tax exposure from IR35** remains outside of tolerance. HMRC raised protective assessments covering the three years 17/18 to 19/20 totalling IRRELEVANT Post Office has appealed the assessments, discussions are actively taking place. A project is in place to re-assess the history of colleagues IRRELEVANT but this will take some time. The impact of the risk is critical due to the fact that Post Office may incur costs of IRRELEVANT (tax costs) and up to IRRELEVANT (penalties and interest. Remediation plan remains off-track.

5. People

- The risk of IRRELEVANT It has been agreed that Post Office will not be taking a 'big bang' approach for the existing population of IRRELEVANT basis. Of 341 contractors in IRRELEVANT of the total population are currently IRRELEVANT of the population are over the IRRELEVANT tenure service. The risk is expected to reduce in IRRELEVANT IRRELEVANT IRRELEVANT
- Risk of **Adverse impact on people's wellbeing** remains outside of tolerance. This is as a result of the ongoing media coverage, increasing workload to support the inquiry, and the volume of work exceeding the resource capacity of the organisation. This all continues to impact wellbeing. Currently the remediation plan remains off track.

6. Enterprise Governance

- The risk **Ineffective Enterprise Governance** has increased from 8 to 12. This is a reflection of the heightened pressure on Co Sec due to the impact of the public inquiry increased requests of FOI and Inquiry requests. The team are stretched to capacity and, whilst Co Sec continue to administer the corporate governance framework, there is no opportunity for reflection and continuous improvement.

7. Data Governance

- Risks **Inadequate Data Governance for unstructured data** and **Inadequate Data Governance for structured data** remain outside of tolerance. Risks have recently transferred over to the Interim Data Management Director (Chris Russell). The remediation plan is currently being reviewed and whilst this will have a short term impact on delivery, there is still confidence that IRRELEVANT maturity can be delivered by 2027, though this is dependent on some limited additional funding being secured in 2025/26/27. The IRRELEVANT opex funding agreed for 2024/25 is for staffing costs only. A plan of what can be achieved over the next two years will be presented to the ARC separately by Chris Russell.

Risk Deep Dives

8. **Retail & Franchise** – We have performed the scheduled 6-monthly risk deep-dive for Retail & Franchise. Risk deep-dives focus on all 3 levels of risk within the business unit - enterprise, intermediate and local risks, after which risk assessments are released, and risk owners are required to update and review risks. All 9 intermediate risks have been reviewed with the senior leadership team. 1 risk was retired, 5 risks are outside of appetite, but within tolerance, and 2 risks are outside tolerance (detailed in Appendix 1) and 2 risks are within appetite.
   - **Emerging risks** which are currently being reviewed; i) Compliance in branch ii) how reactive and support procedures in place support the impact of robbery/burglary in branch iii) Consumers will be disadvantaged or may suffer detriment (customer experience)

- **Inability to improve Branch Profitability -** Risk score remains unchanged (I4:L3). Risk is outside of tolerance. **Program progress**: Network Strategy Acceleration program is making progress, delivering over IRRELEVANT in annualized savings by March 2024. Network numbers remain robust, with over 11.8k branches (including nearly 600 D&C) in March '24, blueprint branches have lower churn (c.3.4%) compared to non-commercial branches (5.4%). **Remuneration Prioritisation**: £30 million package for 2024/25 was announced in March, which should help offset trading challenges and increase income allocation to remuneration. **Next Generation Solutions**: Tender for next-generation SSKs issued in early April, on track for deployment from late 2024/25 (subject to IT dependencies and SPMP business case funding). **Commercial Excellence**: Over 13.5k Commercial Excellence visits completed in 2023/24, now embedded as a BAU practice for Area Managers. **Outlook** Despite remediation efforts, rising cost pressures and limited remuneration growth suggest that branch profitability risks are unlikely to materially reduce in the foreseeable future.
- **Inability to identify, investigate, resolve and treat discrepancies with fairness in the network** – Risk score remains unchanged (I4xL5). Risk is outside of tolerance. **Program progress**: Lottery exit complete we are monitoring the impact to transactions corrects which should decline, note counters to be rolled out to 2,781 branches by 10/24, auto stock rem pilot will commence in June. **Renumeration incentive**: communicated to Postmasters, the first payment of which will be made in their September Remuneration. **BAU process**: revision of the Ops Manual is due to be issued to branches in May, revision of the branch support framework in progress, end to end Dynamics discrepancy tracking, and Branch on a Page reporting has been implemented, improving the Management Information and Insights provided to the business in order to drive further actions which will reduce the volume of discrepancies. **Outlook:** Remediation efforts to mitigate this risk are advancing, and retail remain steadfast in ensuring that our actions across all remediations result in fair and consistent treatment for our postmasters. This commitment aligns with our strategic objective of rebuilding trust. However, the size and sustainability of improvements maybe limited without additional resource, future funding has been requested through the SPM project in order to facilitate a healthy network and support a successful NBiT implementation.

Conclusion: The retail team oversees a total of 64 risks, with 7 pending risk assessments. Currently, the distribution of these risks is as follows: Accepted Risks: 54% Mitigated Risks (with plans to further reduce residual risks): 42% Awaiting Assessment: 4%. To improve risk management. Risks have been realigned to the Retail Assurance Universe, connecting them to relevant controls within our risk tool.

Key Actions and Considerations:

- **Alignment of Assurance Report**: We recommend first line align the actions from the assurance report to determine the actual risk position. Specifically, assess whether the first line has considered these actions and recommendations within the residual scores.
- **Control Effectiveness**: The risk owner's assessment of control effectiveness plays a crucial role in risk reduction. Early findings from SNOW GRC indicate that 29 risks are effectively mapped to controls managed within the risk tool (separate from control issues identified within the Assurance report), 23 risks have a control effectiveness of effective thus reducing the risk, this conclusion has been determined by the risk owner with the current information in the risk tool.

- **Holistic Approach:** By integrating assurance findings, control monitoring, and risk recording, we aim to enhance the overall Retail risk posture while streamlining processes.

Change Spend Review 24/25

9. Change spend review has been agreed for 24/25 which supports remediation of several intermediate risks in appendix 1 within currently agreed funding levels. We will work through potential future funding options over the next 6 months, and will factor into this work the intermediate risks which still require funding to be agreed, these risks are:

- Risk of Non-compliance with Statutory & Regulatory Requirements
- Inability to either retain or attract Legal talent
- Inadequate Data Governance for unstructured data
- Inadequate Data Governance for structured data
- End of Horizon support Agreement
- Branches unable to process Paystation transactions
- Tax exposure from IR35

Emerging Risks

10. While the Horizon replacement has been in progress for some time, the associated risks are managed through the program. However, to enhance operational visibility and assess potential impacts on the Post Office's strategic technology transformation, upon agreement of ownership in first line we will raise and track an intermediate risk. This risk assessment should cover aspects such as strategic alignment with spending objectives, value for money, affordability, achievability, and separation from past practices.

Policy Exception Notes

11. When the business is not compliant with a Post Office Policy, a Policy Exception needs to be raised. These exceptional circumstances should not be considered a normal part of business. The exception should be formally documented as a Policy Exception Note (PEN) and approval obtained from the accountable business sponsor. Currently, there are nine active PENs (please refer to the reading room). Six of these PENs are within the NBiT program for the release of version 2.1, and the expansion to operate in five DMBs is contingent on RMG approval. The programme will ensure that the timelines to gain approval from RMG are adhered to. To maintain visibility and track progress in resolving outstanding actions related to the PENs, the program engages impacted business areas along with the Head of Risk in scheduled fortnightly meetings.

Risk Appetite

12. **Strategy Risk Appetite statements**. We seek approval of the proposed Strategy Risk Appetite statements in Appendix 2**.** These statements will ensure that risks impacting our strategic priorities are managed effectively. For instance, they address issues related to strategic planning, execution, and maintaining shareholder confidence in our strategic vision.

13. **Environmental risk appetite statements**. We seek approval of the proposed appetite statements in appendix 3. These statements will ensure that risks impacting our ability to integrate climate considerations into our business strategy, as per the requirements of the Taskforce on Climate-related Financial Disclosures (TCFD) and SECR streamlined energy and carbon reporting. A detailed report will be presented to the ARC by Mark Cazaly and Martin Hopcroft.

Next Steps & Timelines

14. "Deep Dive" risk review with Technology & Finance will take place in readiness for the June 2024 RCC.

Appendix 1: Intermediate risks outside of Tolerance for May 2024

Enterprise Risk: The Central Risk team have provided a RAG rating, which is our current view of whether remediations plans are on track to the agreed target date.

- 23 risks are outside of tolerance which remains the same as March RCC, please note that the table below includes the **reputational** risks which we do not have an approved appetite in place but due to the high scores this should be reported within this pack.
- 22 risks are outside of appetite but within tolerance decreased 24 to 22 – please refer to the reading room
- 18 risks are within appetite which has decreased from 21 – please refer to the reading room
- 14 risks do not have agreed appetite statements – please refer to the reading room.

#	Enterprise Risk	Intermediate Risk	Latest Management Update	RAG Rating
1	Commercial (5:2) Owen Woodley	RK0020822 - Long term Commercial sustainability of Post Office (4:4) Barbara Brannon	PO has launched a range of new Mails products over the past two years and IRRELEVANT However the market remains extremely challenging with low margins. Due to funding constraints our ability to develop, market, and launch entirely new products is not a current priority with focus on PO core products to reducing costs/maintaining our market share. Change investment spend, IRRELEVANT subject to business case agreed	March 2025
2	Commercial (5:2) Owen Woodley	RK0020697 - Increasing money laundering through banking products (4:4) Ross Borkitt	There is evidence that customers are now using multiple accounts to deposit money, making it harder to identify potential money laundering. There is a further all-hands industry meeting hosted by the FCA on 23rd April 2024.	December 2024
3	Legal (5:3) Ben Foat	RK0021770 - Risk of Non-compliance with Statutory & Regulatory Requirements (5:3) Jonathan Hill	FOIA/DSAR requests continue to increase. Post Office is unable to comply requests within statutory timeframes. IRRELEVANT approved in Opex Committee in March 2024 funding has now been agreed for this from RU/Inquiry to fund increased resource needed for FOIA/DSAR.	October 2024
4	Legal (5:3) Ben Foat	RK0021765 Inability to either retain or attract Legal talent (4:4) Sarah Gray	There is insufficient resource within the legal & investigations team to support the business to manage legal risk and conduct investigations in a timely manner.	June 2024
5	Legal (5:3) Ben Foat	RK0021767 - Poor business planning / Sub-Optimal engagement by the Business of the Legal function (4:3) Sarah Gray	Poor data management and governance creates significant challenges in complying with disclosure requirements. Group General Counsel	June 2024
6	People (3:4) Karen McEwan	RK0021874 - Adverse impact on people's wellbeing. (4:5) Tim Perkins	Due to the recent changes with the People team, this risk will now be owned by Tim Perkins. Ongoing monthly meetings have been planned to continue to monitor this risk commencing April	January 2025
7	People (3:4) Karen McEwan	RK0020647 IRRELEVANT (5:4) Tim Perkins	It has been agreed POL will not be taking a 'big bang' approach for the existing population of IRRELEVANT and will review on a 'case by case' basis.	April 2025
8	Operational (4:3) Martin Roberts	RK0021792- Inability to identify, investigate, resolve and treat discrepancies with fairness in the network (4:5) Mel Park	Operational excellence programme in flight, focus on BAU improvement activity, note counter trial, auto stock rem pilot, risk is expected to reduce January 2025 Operational Excellence: IRRELEVANT agreed Auto Stock Rem IRRELEVANT agreed	March 2025
9	Operational (4:3) Martin Roberts	RK0021791 -Inability to improve Branch Profitability (4:3) Martin Edwards	Re-shape the network in line with our target blueprint to shift towards more sustainable branches, supported by the investment in the 'Network Strategy Acceleration' continuous improvement programme and Network Maintenance "pot" of spend for "right size"/shape of network Auto Stock Rem – In programme is expected to deliver reduction in Postmaster back office hours, increasing profitability Network Strategy Acceleration: IRRELEVANT agreed Network Maintenance: IRRELEVANT agreed	March 2025
10	Security (5:3) Chris Brocklesby	RK0021056 - Inability to prevent Cyber or ransomware attacks (5:3) Neil Bennett	Target maturity has provisionally been set to [redacted] Initiated a Cyber programme which aims to achieve this new target by the end of 2026. A new CISO started on 18 March and is assessing current position and will confirm target maturity and dates. IRRELEVANT agreed for 24/25 agreed	December 2026
11	Security (5:3) Chris Brocklesby	RK0021055 Inability to recover from a Cyber attack (5:3) Neil Bennett	Target maturity has provisionally been set to [redacted] Initiated a Cyber programme which aims to achieve this new target by the end of 2026. A new CISO started on 18 March and is assessing current position and will confirm target maturity and dates. Funding agreed as above	December 2026

#	Enterprise Risk	Intermediate Risk	Latest Management Update	RAG Rating
12	Information (3:3) Tim McInnes	RK0021709 - Inadequate Data Governance for unstructured data (**4:4**) Chris Russell	Funding agreed IRRELEVANT opex This funding is not sufficient to reduce the risk. Without further investment POL will not be able to implement a robust, sustainable and scalable solution for Data Governance.	March 2027
13	Information (3:3) Tim McInnes	RK0021710 - Inadequate Data Governance for structured data (**4**:3) Chris Russell	Funding agreed IRRELEVANT opex This funding is not sufficient to reduce the risk. Without further investment POL will not be able to implement a robust, sustainable and scalable solution for Data Governance.	March 2027
14	Technology (5:4) Chris Brocklesby	RK0021876 Legacy Data Infrastructure (**3**:4) Wilson Gill	MDM Credence Upgrade costs IRRELEVANT agreed Data Enablement Programme IRRELEVANT agreed	March 2027
15	Technology (5:4) Chris Brocklesby	RK0020077 - Suboptimal Belfast datacentre resilience levels (5:3) Simon Oldnall	Current refresh programme will be substantially completed by March 2025. Data Centre Fortification (Hybrid Funding) - IRRELEVANT agreed Horizon Defect Remediation **(DBT Funding)** IRRELEVANT agreed **DBT Funding amounts are subject to business case approval from DBT**	March 2025
16	Technology (5:4) Chris Brocklesby	RK0021031 - End of Horizon support Agreement (5:3) Simon	Formal discussions commenced with FJ on extension beyond March '25 for a period up to 5 years. Signing of the contract is planned for October 24. Horizon Contract Extension **(DBT Funding)** £1.8M **DBT Funding amounts are subject to business case approval from DBT**	October 2024
17	Technology (5:4) Chris Brocklesby	RK0020673 - Inability to Support & Maintain elements of Accenture Back Office Platform (**4**:3) Paula Jenner	Original assessment was that the risk would reduce by March 2024 the risk requires a reassessment to consider the programme to remediate. Back Office Operational Modernisation - IRRELEVANT agreed	TBC
18	Technology (5:4) Chris Brocklesby	RK0020816 - Inability to trade should the full network of Post Office branches not be migrated from copper to fibre-compatible **(5:3)** Paula Jenner	Challenges within the project and BTs programme. These challenges are starting to impact on the programme planned schedule, although we are still planning to complete in Dec 2025. The risks in the programme are actively being discussed and plans for mitigation are being actioned.	December 2025
19	Technology (5:4) Chris Brocklesby	RK0022291 Branches unable to process Paystation transactions **(4;3)** Simon Oldnall	Second device programme is the remediation for this risk, the programme status is currently red. Investment committee approved spend until the end of June to purchase hardware and continue development.	March 2025
20	Finance (5:3) Kathryn Sherratt	RK0020025 Inability to implement compliant health & safety processes across the business (5:3) Martin Hopcroft	Processes and procedures are in place to effectively mitigate risks in relation to colleague safety and physical security practices	December 2024
21	Finance (5:3) Kathryn Sherratt	RK0021857 Tax exposure from IR35 **(5:4)** Tom Lee	HMRC correspondence in recent months states their position and they have issued a protective assessment letter, next steps are currently being worked through.	TBC
22	Reputation (3:3) Catherine Cool	RK0021078 Lack of public trust due to historical issues (**5:5**) Simon Marshall	In (FYE) Q4 we saw a sharp drop in brand trust as a result of the ITV drama in January 2024. We saw a slight improvement in February, and this also continued into March 2024. However, we will not be able to determine the net loss in brand trust until the same period in 2025	December 2024
23	Reputation (3:3) Catherine Cool	RK0021013 - Uncertainty to Post Office Brand Commercially **(4:4)** Simon Marshall	Engagement with the relevant stakeholders across the business to include both the short-term and longer-term impact to identify plans to reduce risk	December 2024

Appendix 2 – Risk Appetite - Strategy

Risk Themes	Risk Appetite Statement	Risk Appetite	Risk Tolerance
1. Failure in strategic planning and execution	IRRELEVANT		
2. Failure to maintain shareholder confidence of strategic vision			

Appendix 3 – Risk Appetite - Environment

Risk Themes	Risk Appetite Statement	Risk Appetite	Risk Tolerance
1.Ineffective Environmental strategy – transitional risk	IRRELEVANT		
2.Physical Impact of climate change - (PO Branches) – physical risk			
3. Physical Impact of climate change - (PO Sites) – physical risk			
4. Inadequate Sustainable Suppliers – transitional risk			

3.2

POST OFFICE LIMITED

AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Group Compliance Update	**Meeting Date:**	21st May 2024
Author:	Jonathan Hill, Group Compliance Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting

The Committee is asked to:

Note the Group Compliance update, particularly:

- The ICO's decision to issue a Practice Recommendation to Post Office, following the decline in our compliance with response timescales.

POL Compliance Status/Overview

*Please note Group Compliance does not oversee all areas of the business.

1. The areas in which we continue to identify potential and emerging risks are:

Data Protection & Information Rights

(i) FOI requests

Since the start of 2024 there has been a huge increase in the number of FOIs received, leading to a drop in completion timelines. For context, POL has received 299 FOIs since 1st January 2024, compared to 104 FOIs for the same period (1st January – 29th April) in 2023. The complexity of FOI requests has also increased, with requesters asking for very specific information about prosecution/conviction data, financial records and about branch closures. We have also seen an increase in FOIs about specific individuals as a result of recent evidence at the POHIT.

We met with the ICO on 30th April, and due to concerns the ICO has with Post Office's compliance with FOI timescales, it will issue a Practice Recommendation ("PR") around mid-May. The PR is a support tool used by the ICO to recommend steps for a public authority to take to help improve its compliance with the FOI Code of Practice. It is a lower level than an Enforcement Notice and we expect it will recognise the proactive engagement we have established with the ICO and the steps already taken to manage the unique circumstances Post Office is going through. We are responding to the ICO's initial questions to help them draft the PRs. The ICO publishes details of PRs served to public authorities on its website and we expect this to happen around mid-late May. It is considered likely that the ICO will take similar action regarding Post Office's compliance with data protection legislation and will issue a further PR covering Information Rights. We will continue to meet with the ICO every two months.

We continue to raise sensitive cases with the SEG to ensure awareness, most of which pass without comments.

We have had 4 new vacancies approved for the FOI Team and we are currently working with the Talent Acquisition Team to recruit new members.

(ii) Data Protection Requests (including Data Subject Access Requests (DSARs))

We continue to experience a significant surge in applications for DSARs, with 285 cases outstanding as of 13th May 2024. Most relate to HSS (235). To illustrate the surge, between 1st January and 29th April 2023 there were c.125 requests compared to c.413 in 2024. With the Select Committee and upcoming phases of the Inquiry, the surge is expected to continue. It is also worth noting that the requests being received are significantly more complex than the majority of those received in 2023. We are working on a resource plan to close these cases with the RU team in addition to the 4 additional roles already approved.

On a positive note, the ICO has stated that there is no further action required in relation to a DSAR complaint and that the individual had been provided with the information to which they were entitled.

(iii) GLO Scheme

The project team is continuing the delivering of disclosure material and hitting the target for cases each week.

We continue to meet regularly with the ICO, with the ICO remaining supportive of the work that Post Office is undertaking with regard to Information Rights requests and commented on the continued resilience of the teams, however we are anticipating more complaints to the ICO due to the ongoing delays.

(iv) HSS

Delays in responding to DSARs connected to existing and new HSS applications are impacting on the HSS and Dispute Resolution teams, as they are unable to progress some cases. [redacted]

(v) AWS Data Breach ("Over-permissioning" of Access)

A data breach was communicated to over 70 clients mid-March relating to potential access to client personal data from two suppliers based in India (a 'data transfer'), which is contrary to data protection law and client contractual requirements. The personal data was contained within several 'S3 buckets' that were established to merge and split files coming to and from clients in preparation for parallel running with of both NBIT and Horizon.

It is understood that at least three clients (including POI) reported the unlawful data transfer to the ICO. The Data Protection team attended 11 calls with clients and responded to 200+_ questions. A Root Cause Analysis document is being released to clients in early May. The risk is that the incident has reduced client confidence in Post Office's ability to deliver NBIT and will result in heightened scrutiny of the future roll out.

For additional information, see paper submitted by the CISO and Internal Audit, who have been looking at both the incident response processes and the design of the excessive access permissions at the root of the issue.

Financial Crime/AML/ABC

(i) The Fit and Proper Remediation Prove Case

An IT Solution Design Review was held with key senior stakeholders. The key outcome was that the business should restructure the project delivery to prioritise compliance risk reduction, consider a need for broader Business Process Re-engineering to fully evaluate upstream business process issues which impact CDP F&P (out of scope) and develop a 3-phased delivery approach to deliver the biggest reducers of compliance risk first, within approved funding. The F&P SteerCo has agreed to go ahead with the phased approach and re-engage Accenture to deliver Phase 1. The re-engagement with Accenture is underway and currently focusing on planning the data re-baseline (to resolve historic data corruptions) and new exception handling processes.

(ii) Economic Crime and Corporate Transparency Act 2023 (ECCTA)

Key stakeholders across the business have been identified and approached to set up the ECCTA working group. A draft Terms of Reference has been shared and will be agreed by the working group. The aim is to undertake and document a risk assessment and review of current processes and procedures, identify key areas of risk for POL and document proposals to address those areas of risk, along with relevant owners of any actions. An initial report will be prepared for the SEG by end May 2024. The working group will be acting swiftly in order to identify risks and strengthen controls before the new failure to prevent fraud offence comes into force, which will be after the UK government publishes guidance on what constitutes reasonable procedures to prevent fraud, it is anticipated that this could be in late 2024.

(iii) FCA Roundtable – Cash Deposits at PO

On the 23rd April, the FCA hosted a roundtable with the National Economic Crime Centre, the National Crime Agency and Post Office Banking Framework Partners (BFP's) regarding cash-based money laundering. Mandatory cash deposit limits at Post Office counters has positively impacted the economic crime landscape and imposed tougher measures for criminals to launder proceeds of crime through the Post Office network. The taskforce has not been able to fully assess the impact of the change, however, BFP's & the NCA have seen a notable change in suspicious activity since the introduction of the new deposit limits.

The FCA has indicated that it will now shift its regulatory focus on other cash-based money laundering risks, such as cash deposits at Paypoint, and will maintain a degree of oversight for Post Office everyday banking activity. It is anticipated that Post Office will, as a result of its network and service coverage, continue to be exposed to high-volumes/high-values of money laundering risk. The Financial Crime Team has recently launched the annual AML training campaign and continues to work with internal and external stakeholders to raise awareness of risk and frequently assess the risk of money laundering at Post Office counters to improve prevention, detection and correct controls.

(iv) HMT MLR Consultation

On 11 March, HM Treasury published a consultation entitled "Improving the Effectiveness of the Money Laundering Regulations" and closes on the 9th June 2024. In 2022, the Government reviewed the anti-money laundering/ counter-terrorist financing (AML/CTF) regulatory and supervisory regime and its Economic Crime Plan set for 2023-26. The Government has now extended its aim to improve the effectiveness of the current Money Laundering Regulations 2017 (MLRs) and will assess three strands of legislation (proportionality and effectiveness of customer due diligence, the effectiveness of public body/supervisor coordination and extending the scope of the MLRs for unregulated firms (i.e. crypto providers)).

An initial review suggests that Post Office is unlikely to be impacted by current consultation, however the FCT are reviewing the consultation questions, fully assessing the impact to Post Office and will report full findings for June RCC.

Financial Services

(i) Mystery Shopping

32 mystery shops were graded below expectation in March (19.9%) - Travel Insurance (32.5%), Savings (8.2%), and Over 50s (5%). An improving trend is noticeable in Savings and Over 50s shops when comparing below expectation grades Q4 v Q3. Savings (Q4-15.2% Q3-18.2%), Over 50s (Q4 – 3.1% Q3 – 33.3%). 8 Travel Insurance shops were impacted by branches using the new leaflet too early rather than not following the sales process. If these are discounted the below expectation percentage would have been 22.5%.

109 Branches were re-shopped in Q4 after failing a shop. 19 of these failed their second shop, evidencing that the quality of plans is improving.

Conduct Compliance review improvement plans completed by Area Managers following a failed shop and provide feedback to improve quality. Where a branch fails a second shop this is escalated to the Regional Manager to investigate.

Further discussions are taking place to agree a process to permanently withdraw a product from a branch following 3 failed mystery shops.

From April mystery shop reporting will change to align with how POI report. The percentage of shops where the sales process has been able to be tested and passed will be reported rather than the percentage of total shops.

(ii) Compliance Oversight

Conduct Compliance has reviewed the work it currently carries out and has produced a RACI matrix across Post Office business areas to align work to the first line where appropriate. This has been shared with affected business areas for comment and is currently with POI as the lead Principal to review and revert back to Conduct Compliance w/c 6th May.

(iii) Consumer Duty

The FCA set higher standards for consumer outcomes and introduced the Consumer Duty regulation on 31st July 2023. To achieve this, it has introduced a new principle ‘A Firm must act to deliver good outcomes for retail customers”.

To gain assurance that products sold in branch and online are meeting Consumer Duty regulations Conduct Compliance have discussed with the Principals who have confirmed that appropriate steps have been implemented.

Appendix 1 - Status of Group Compliance Activities

The table below provides a status of 2023/24 Group Compliance Activities:

Activity	2023/24 Group Compliance Activities	Status of Group Compliance Activities	Current Compliance Results	Comments
Group Policy Compliance	Policy reviews to be restarted in Q3 2023/24	●	TBC	We have restarted the Group policies annual compliance review cycle with the first reviews to be Quality Assured by the Assurance and Compliance directors before being issued
FS Mystery Shopping	c160 shops were carried out in 23/24 (excl. Dec)	●	●	32 mystery shops were graded below expectation in March (19.9%) - Travel Insurance (32.5%), Savings (8.2%), and Over 50s (5%). An improving trend is noticeable in Savings and Over 50s.
Data Protection and Information Rights	Accountability Framework planned actions for 2024.	●	●	A Data Governance Framework has been agreed with Post Office and all teams in Post Office are working to get to Level 2 maturity
Financial Crime	30 Risk assessments completed, 7 assessments in progress in Q1 2024/25	●	●	Identity Services, Money Transfers and Travel Mony were assessed in March and the services have been reported as medium risk with no significant findings or emerging/increasing risks to report. Annual risk assessments for Anti-Bribery and Corruption are currently underway for completion by 30 April. New products/changes are prioritised with continued regulatory landscape monitoring for emerging risks.
Financial Crime	Quarterly policy assurance for AML/CTF, ABC & FC policies and HMRC F&P policy.	●	●	Assurance against minimum control standards remains amber due to ongoing issues with Fit & Proper agent data and current manual workarounds and occasional instances of G&H non-conformance. Funding has been approved to implement 9 data and system changes identified by the F&P Project, which will be delivered over the next 12 months.
Supply Chain	22 reviews complete to the end of March 2024, three were joint CViT and Processing site	●	●	The average results of Supply Chain assurance reviews decreased to 3.5 at March 2024 from 3.88 in January 2024

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

3.3

Title:	Group Assurance Update	Meeting Date:	21st May 2024
Author:	Anshu Mathur, Group Assurance Director	Sponsor:	Sarah Gray, Interim Group General Counsel

Input Sought: Noting

The Committee is asked to note and discuss the Group Assurance (GA) update, particularly:

- Status update on Legacy Matters Continuous Assurance and associated risk(s).
- Status of Management Open Actions.

Group Assurance (GA) - Status / Overview

1. Legacy Matters Continuous Assurance

The status of the control environment for those business functions captured within Continuous Assurance, as at 10th May 2024, is summarised in the table below:

Q1	10th May 24	Functional activity progress			Group Assurance opinion			Overdue Actions Status			
Business Area	Activity	Current	Previous*	Movement	Current	Previous	Movement		Current	Previous	Movement
Retail	Function self assessment	25	14	⇧	■	■		Thematic	9	7	⬆
	GA assessment sample checks	0	0		░	■		CIJ/PM Policy	57	17	⬆
	GA assessment	33	14	⇧	░	■		QAF	10	14	⬇
LCAS A&CI incl Speak Up	Function self assessment	16	6	⇧	▨	▨		Speak Up	1	1	⇔
	GA assessment sample checks	0	2		░	▨					
	GA assessment	15	5	⇧	░	▨					
Assurance Reviews	Non-Detriment review		░		░						
	Overturned Convictions Review		░		░						
	Past roles assurance		▨		▨						

Legend ■ Unsatisfactory ▨ Satisfactory ▨ Improvement Needed ░ WIP - GA Opinion TBC

**Previous figures for 'Functional activity progress' reflects activity from Q4 (Jan-Mar 24)*
Q1 Continuous Assurance activity includes P1 and P2 risks, and are reflected in the 'Current functional activity progress'.
Previous Q4 Continuous Assurance activity only reviewed P1 risks.

Continuous Assurance

Continuous Assurance continues embed across the various functions. The outcomes of assurance activities range from Green to Red, which reflects the divergence in the complexity of the functions involved and pace at which functional self-assessment is embedding becoming BAU.

- **Retail**
  a) Retail responses to GA request for information and self-assessment has greatly improved this quarter, however the quality of artefacts sent still needs attention.

  b) GA are now asking each function **if they consider their controls/mitigations are sufficiently robust to manage risk**. This question is ensuring the function lead understands that it their responsibility to provide first line assurance over the controls/mitigations.

  c) Overdue open management actions remain significantly high and only **16%** (13 out of 83) actions closed to date. The significant increase since the last ARC is driven by 36 PM Policies actions now overdue with a reforecast closure date of June 2024 for majority of these.

3.3

Risk

  - In our opinion the status of Retail's Functional Assessment (Continuous Assurance) and level of open management actions have a direct correlation on Retail's ability to demonstrate their conformance with common issue judgement and impacts of actions delivered particularly to Postmasters.
  - Whilst engagement and communication between GA and Retail is continually improving and we can see Retail moving in the right direction, i.e., changing their approach to self-assessment and beginning to proactively challenging artefacts before sending to GA, these improvements will take time to embed through Retail and trickle through to the dashboard.

- **A&CI**

  Engagement with A&CI is exceptional with self-assessment fully imbedded and quality of artefacts to demonstrate their control environment is robust.

- **Culture and RU**

  Since April 2024 we are engaging with Culture and Remediation Unit to commence their self-assessment, and we anticipate the outcomes of these activities should be included in our Group Assurance dashboard from Q2.

Please refer to **Appendix 1** for a detailed summary of Management Open Actions.

Appendix 1 - Legacy Matters – Status of Open Management Actions

The status of all Open Management Actions as at 10 May 2024 is summarised in the table below:

			Of the open actions:		
Management Actions / recommendations from Assurance Reviews	**Function**	**Open**	**Current**	**Overdue < 3 mths**	**Overdue > 3 mths**
Speak Up	LCAS	1			1
Common Issues Judgement	Retail	3	1	8	22
Postmaster Policies	Retail			36	
Quality Assurance Framework (QAF)	Retail	4		6	4
A&CI	Various	4	4		
Grand Total as @ 10/05/24		**12**	**5**	**50**	**27**
Grand Total as @ 11/03/24		**112**	**73**	**29**	**10**

As evident from the table the overdue profile has significantly deteriorated since the last ARC in March 2024:

Retail

The number of overdue actions has significantly increased significantly in April 2024 primarily due to Postmaster Policy Review actions which became due 31 March 2024. It should be noted that a re-forecast closure date for majority of these is 30 June 2024.

Of the 70 Retail overdue management actions, excluding QAF, the movement in the period can be summarised as follows:

- No change – 34* (driven by PM Policy actions)
- Update received but no evidence provided – 3
- Evidence received and being assessed – 11
- Evidence received but still overdue as evidence is not to the standard required – 7
- Evidence received for part of the action(s) and assessed – 5
- Action to be moved to another business function – 2
- Re-forecasted dates for closure – 8

Quality and frequency of engagement / updates between Retail and GA are beginning to improve, with the focus on Retail being able to self-assess efficacy of the artefacts before these are forwarded to GA for review and closure.

A&CI/Speak Up

One Speak Up action continues to remain open and is dependent on the Speak Up strategy, which is in its final stages of approval, in the meantime, awareness work is progressing.

Four A&CI recommendations remain open, the recommendations are reliant on various areas of the business to complete actions, and this may cause delays.

3.3

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Title:	SPMP Integrated Risk Assurance Universe	Meeting Date:	21st May 2024
Author:	Anshu Mathur, Group Assurance Director	Sponsor:	Sarah Gray, Interim Group General Counsel

Input Sought: Approval

The Committee is asked to:

- **Approve** the additions made to the SPMP Integrated Risk Assurance Universe.
- **Note** the status of the SPMP Assurance Reviews.
- **Approve** the 34 Statement of Works.

1. SPMP Integrated Risk Assurance Universe – For Approval

In the period since the last ARC in March 2024, we have made the following changes to the SPMP Integrated Risk Assurance Universe:

- **Governance Pillar**
  Based on feedback from the GE SPMP Sub Committee in March 2024, we have now added 4 P1 risk lines/items to capture Business Case (BC) and Benefit Realisation (BR) Assurance. As a consequence the Governance pillar has 21 risks vs 17 previously.

  Whilst the Assurance teams (both SPMP and Group) currently do not have the capability to deliver BC and BR assurance, funding has been secured to recruit.

The SPMP Integrated Risk Assurance Universe therefore comprises 509 (previously 505) inherent risk spread across 16 pillars. Please refer to **Appendix 1** for the current snapshot of the SPMP Integrated Risk Assurance Universe.

2. Statement of Works (SoW) - Approval

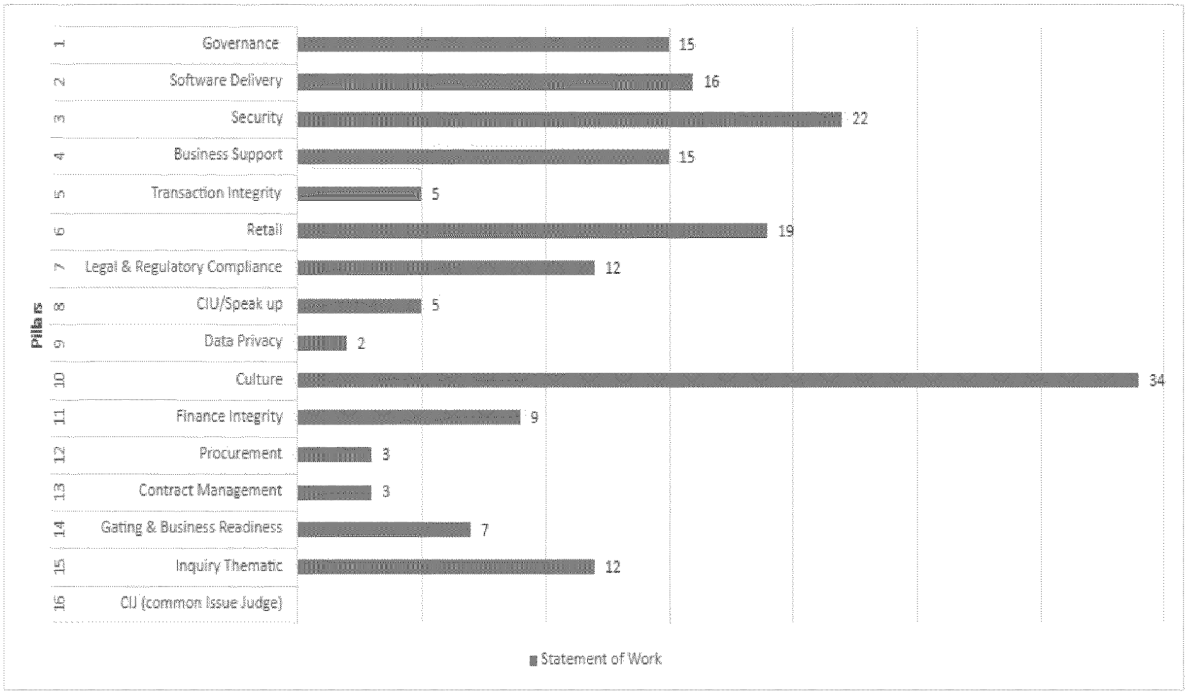
As mentioned in the ARC in March 2024, we have now completed drafting 34 SoW defining the assurance scope and coverage of risk lines. As shared with ARC, we have applied the following principles to determine the coverage and scoping of SoW:

- Adequate coverage of material key risks (P1's, where appropriate P2's and P3's).
- End to End assurance to provide a programme and business view of readiness.
- Assurance coverage across pillars to ensure efficiency and eliminate rework, if possible.
- Clear assessment of Postmaster protection and or KRI's.
- Adequacy of design (where applicable – effectiveness) of Controls.
- Identify SoWs that may need periodical refresh, contingent on release strategy.
- Coverage and mapping of HIJ and CIJ.

By applying the above principles, we have ensured adequate coverage exists not only from a pillar perspective but also from an inherent risk lens:

- **Pillar coverage** - The table below demonstrates that the 34 SoWs touch all 16 pillars:

Coverage of SoW per Pillar



A few key things to note are:

- CIJ spans across Transaction Integrity, Finance, Security, Retail, Business Support, Data Privacy, Software Delivery.
- Transaction Integrity spans across: Finance, Data, Security, Business Support, & Retail.
- Culture will be a core underpin of all our reviews.

- **Inherent Risk coverage** - The 34 SoWs provide 100% coverage of all the P1.   Please refer to **Appendix 2** which shows the coverage of inherent risk per SoW.

Appendix 3 provides the details of SoW scope and the assurance outcomes. Please note, these SoWs form the initial premise from which assurance work will commenced and are considered draft and not exhaustive, as input will be taken from Business / Programme / SMEs / Stakeholders (internal and external) before finalising the Terms of Reference.

We have not provided anticipated timelines for when these 34 SoW would be delivered, as this is very much contingent on resourcing, capability, allocation of external assurance support, risk profiles of SPMP releases, and the completion of the first 5 SoW.

3. SPMP Assurance Tracker

The table below provides the status update for the 5 SOWs as at 15 May 2024:

	SOW	SOW Ref	Terms of Reference	Fieldwork	Planned Reporting	Planned Completion
1	Business Requirements	SOW 1	April 24	April 24	June 24	June 24
2	Defects and Risk Management	SOW 6	April 24	April 24	June 24	June 24
3	Security / User Access – Account management, access control, audit logging and user access	SOW 5 & 8	April 24	April 24	June 24	July 24
4	Transaction Integrity	SOW 3	May 24	May 24	June 24	July 24
5	Retail Readiness (NEW)	SOW 26	April 24	May 24	June 24	July 24

Legend: Completed On Track Delayed

Whilst progress has been made, we have not in full earnest commenced fieldwork. This is primarily driven by the Assurance Team(s) focus on ensuring all SoW are drafted. In addition, the drafting and finalisation of Terms of Reference were more complex than initially thought and required wider business engagement.

Group Assurance are engaging with the programme to assess whether we continue to have the right composition and capability to deliver the assurance programme. The programme has recently approved to hiring of two assurance resources to support delivery of the assurance programme.

For SoW 5 and 8 (Security / User Access – Account management, access control, audit logging and user access) the SPMP assurance team are engaging with a 3rd party service provider TMC3 who have been brought into look at data breaches by the SPMP Programme management team. The provider at present is planning to conduct a root cause analysis of the 2 breaches identified and the Statement of Work for this Phase is being drafted by TMC3. The functional assurance team will ensure that there are no duplications of assurance through understanding TMC3 scope before executing any detailed work.

We have also, subject to ARC retrospective approval, are planning to commence SoW 26 to focus on Retail Readiness to receive the SPMP platform (both pilot and waves). The ToR for this review will be shared and discussed with the Retail Engagement Director to ensure key operational insights are captured from a legacy perspective.

4. Other Updates

- **Procurement - External Assurance SME Support**

  After the initial pre-market engagement held from February to March - the initial engagement engaged with 10 suppliers, of which 5 remain (PA Consulting, Ernest & Young, Crowe Consulting, Protiviti and Credera).

  A sourcing strategy has been created (informed by market engagement) has been submitted to PDB, Steerco, SEG in May and Board for approval to proceed in June 2024.

  The preferred procurement option would be to release a single FTS procurement but as this would take 4-6 months to complete the plan is to split procurement activity into two phases.

- **Phase 1** Review the current SPMP Integrated Assurance & Risk Universe for completeness and against industry best practice.
- **Phase 2** Create the invitation to tender (ITT) with a detailed set of requirements derived from the universe and a plan for assurance that can be provided to the market, including commercial protections for both the bidder and POL on 'how' assurance outcomes will be presented.

Group Assurance are also working in parallel to create a contingency worst-case scenario where POL may have to create their own internal pool of SME Contractors.

- **Recent external reviews on SPMP**

  For the committees awareness two external reviews have been performed on SPMP, which management are in the process responding to and preparing remedial action plans.

  In our opinion, both reports highlight consistent concerns on the deliverability of SPMP. Key extract from these reports are summarised below:

  - **Infrastructure and Projects Authority (IPA) Draft Report**

    For the Committee's awareness, in April 2024 IPA performed a review on Horizon Replacement (SPMP, SDES, and Horizon Extension), this covered gates 0 to 3 to support a Treasury Approval point of the Programme Business Case for funding between June 2024 and March 2026. Their scope covered:

    - Gate 0 – Looks historically on the delivery of the Horizon replacement programme
    - Gate 3 – Test the maturity and robustness of the Programme Business Case
    - The review also assesses whether governance arrangements across interested and invested oversight and delivery partners remains effective and robust.

    IPA 's draft opinion is as follows: '**RED** - Successful delivery of the 3 POL Programmes that deliver the Horizon replacement to time, cost (defined in the business case under consideration) and quality appears to be unachievable. There are major issues which, at this stage, do not appear to be manageable or resolvable entirely within POL. The programme/project may need re-baselining and/or its overall viability re-assessed.'

    According to their rating guidance – 'This programme/project should not proceed to the next phase until these major issues are managed to an acceptable level of risk and the viability of the project/programme has been re-confirmed.'

    The review identified three strategic issues that could help sustain these high-risk programmes through to successful conclusion:
    (1) Providing clarity of governance, now Horizon replacement is on Government Major Projects Portfolio (GMPP). There is confusion about which of the 3 programmes are coming onto GMPP and this needs to be resolved.
    (2) We are recommending government consider if the financial arrangements are appropriate for these programmes.
    (3) It is the right time for a meaningful conversation about risk appetite as only a common understanding of this across all governance bodies involved, will enable the programme, and especially the technical development of NBIT, to be successful.

    The review recognised that Programme Leadership has been tackling poor quality and weak management controls (especially planning, monitoring, and reporting and proper risk based assurance) and improving quality of technical development. The report has identified 7 recommendations that management are in the process of working through.

- **Public Digital (PD) Report – Final**

  On behalf of DBT, PD have completed a review of SPMP and New Branch IT. The goal of the review was to assess the viability of SPMP in meeting POL's future needs, focussing on POL's capability to deliver the programme, the technical approach being taken, value for money and other factors. Their key observations are summarised below:

  - Whilst trending in a generally positive direction with pocket of excellent work and deeply expert people, SPMP overall is not currently in a healthy place.
  - There are significant gaps in strategy, capability, technology and Governance that need addressing.
  - A high level of management churn along with lack of corporate memory, presents a risk of the past (lessons from previous failed attempt to re-platform) repeating itself.
  - Throwing ever more resources at the problem will not solve the problem.
  - SMPM's viability is being undermined by serious deficiencies in its governance, technical, and implementation approach.
  - The responsibility and accountability to fix the issues does not sit only with the Programme. It will require the whole of POL, and key partners in UKGI and DBT to work together to do this.

  Key findings:

  - The vision and dominant framing of SPMP does not align with an overall POL strategy, is not agreed and understood by the wider POL business, and is not consistently recognised within the SPMP programme
  - The organisation lacks permanent people with critical capabilities and experience, and there is an absence of continuity in keystone functions, particularly in leadership and management, which creates unacceptable risk to the programme.
  - Historical technology choices and development practices, adopted to attempt to meet significantly different past programme goals, have left significant technical debt in the heart of the product. Good practice and standards have now been codified, but are not yet in place across the full delivery organisation.
    - Weighing pros and cons, we concluded that if our review team was leading the project despite the obvious sunk costs we would give very strong consideration to reintroducing an off-the-shelf ePOS solution as the core retail element, while retaining all the integration work that the teams have invested time in.
  - POL's recent history is driving a fear of accountability for decisions, resulting in risk aversion and a governance model unsuited to the need. The programme, business, and wider stakeholder ecosystem must work as "one team" towards shared outcomes
  - The programme is not truly user-centred and the professional practice of "product management" is not well understood inside POL. This has resulted in an inconsistent approach to product development that has become disconnected from delivering value to users.

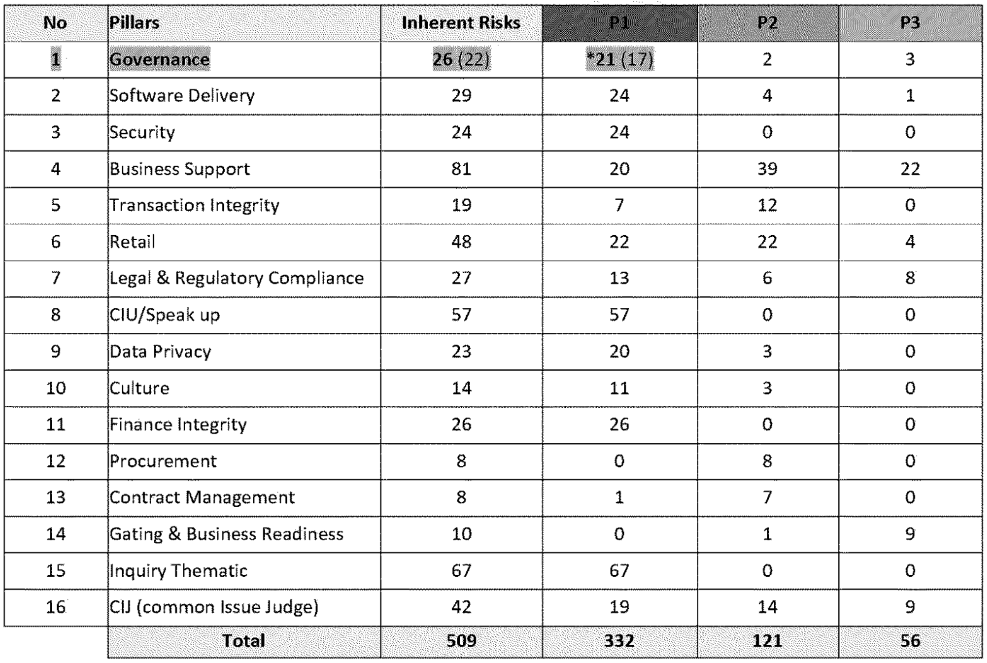
5. Key Next Steps

1. Focus on commencing and completion of the 5 SoWs in flight.

2. Assess adequacy / capability of Assurance resources – June /July 2024.
3. Commence G-Cloud 13 engagement to commence work on Phase 1 of the work required to support assurance - May 2024.
4. Obtain approval from the PDB, Steerco, SEG for the 2 Phased procurement approach - May 24, followed by Board approval at the June 2024 meeting.
5. SPMP functional assurance and Group Assurance to work on a paper to create a plan B for an internal pool of SME Contractors - June 2024.

POL00448733

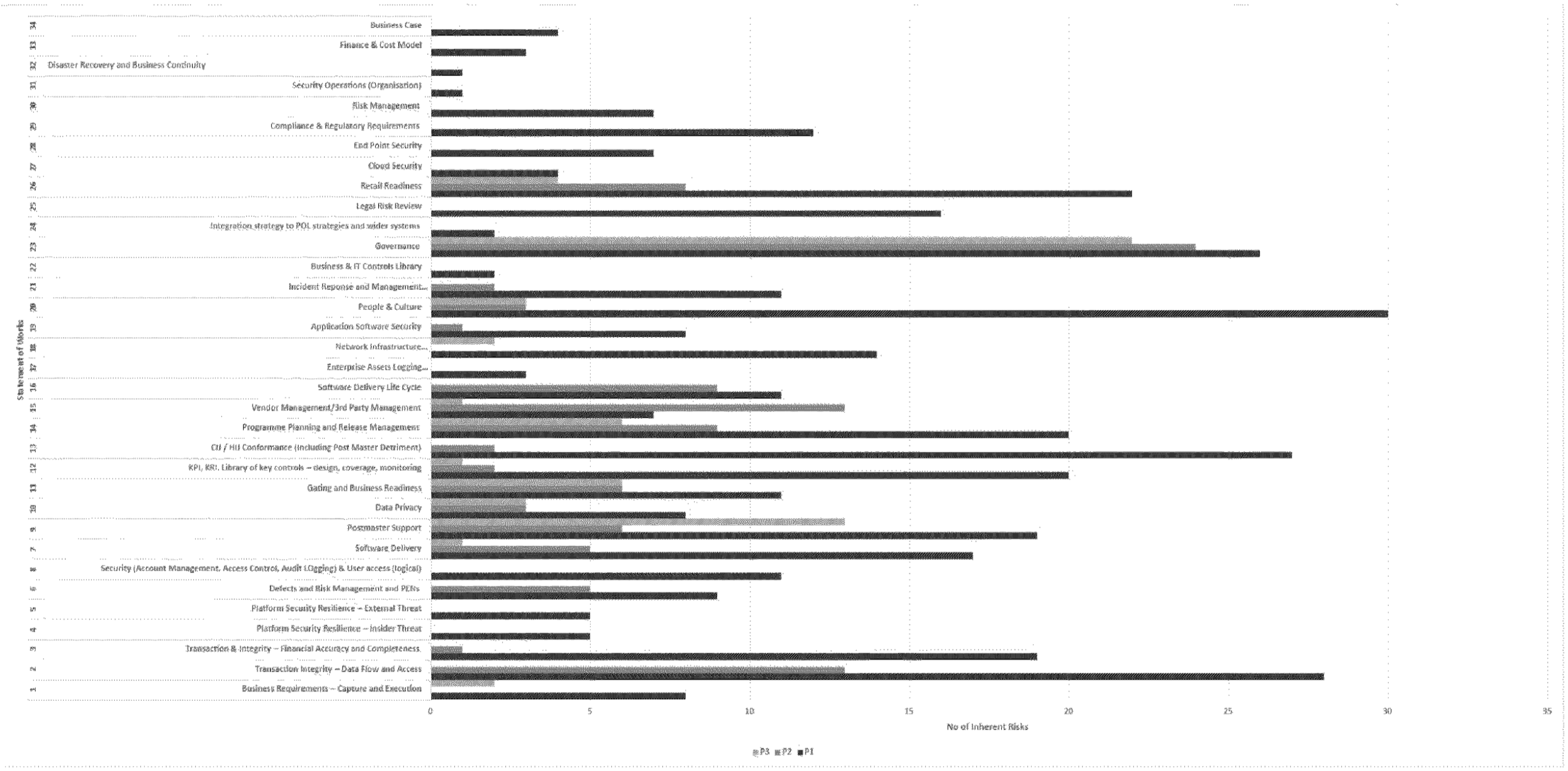
Appendix-1- SPMP Integrated Risk Assurance Universe – 30 April 2024



No	Pillars	Inherent Risks	P1	P2	P3
1	**Governance**	**26** (22)	***21** (17)	2	3
2	Software Delivery	29	24	4	1
3	Security	24	24	0	0
4	Business Support	81	20	39	22
5	Transaction Integrity	19	7	12	0
6	Retail	48	22	22	4
7	Legal & Regulatory Compliance	27	13	6	8
8	CIU/Speak up	57	57	0	0
9	Data Privacy	23	20	3	0
10	Culture	14	11	3	0
11	Finance Integrity	26	26	0	0
12	Procurement	8	0	8	0
13	Contract Management	8	1	7	0
14	Gating & Business Readiness	10	0	1	9
15	Inquiry Thematic	67	67	0	0
16	CIJ (common Issue Judge)	42	19	14	9
	Total	**509**	**332**	**121**	**56**

*Note: Change in the period is highlighted in yellow (prior figure).

Appendix 2 - SoW Coverage of Inherent Risks



Appendix 3 –SoW's – [These will continue to be evolved and updated with business and SME input.]

SOW #	Title	Key Pillars	Scope	Assurance outcome
1	Business Requirements – Capture and Execution	1. Governance 2. Business Support 3. Data	To ensure the programme has implemented a structured methodology for the ownership, capture, execution and change management of Business Requirements. This will be an End-to-End review with a focus on: 1) Compliance with all legal, regulatory, operational, commercial requirements and how featured in the Business Requirements (including HIJ / CIJ considerations). 2) Alignment with the Business Case. 3) Ensure effective translation of the requirements covering Data and Security into the Business Requirements. 4) Document management to support status and amendments throughout the programme delivery cycle. 5) Construct of testing (e.g.UAT) to ensure essential elements of the requirements are proven against deliverables. 6) Effectiveness of governance and oversight. 7) Clearly defined process, controls, reporting and organisation structure (+RACI) to support all the above.	Programme can demonstrate a clear audit trail of requirements, and their lifecycle, including implemented vs not, and oversight. Clear evidence / artefacts provided to support how Business: 1) Requirements were initially captured and maintained /controlled throughout the programme delivery cycles. Including change controls process. 2)Proof that all essential elements of the programme deliverables (e.g. regulatory / data / CIJ /Security, TI etc) have been defined and appropriately sign off. 3) All testing (e.g. UAT) has been aligned with Business Requirements to ensure compliance as necessary. 4) Processes / controls in place, and followed, and aligned with best practice.
2	Transaction Integrity – Data Flow and Access	1.Transaction Integrity 2.Business Support 3.Retail 4.Security	To ensure key data flows are mapped and documented. And to ensure that access to relevant data sets is defined by roles and transactions. Obtain and review the Architectural design and set up of the new platform and the data flow diagrams which sits alongside. Understand ownership and change management protocols. Review the Integration linkages to other systems to ensure these have been identified and defined with dependencies/risks. Understand the Integration plan and testing strategy, including the stage gate sign-offs. Review roles designs and set ups and how these relate to the transaction objects and related information access through these objects.	SPMP has a defined data flows and data set. And that rule sets and roles exist to manage the access and visibility, including security. Clear Architectural design diagrams with supporting data flow diagrams. With clear ownership and accountabilities for the different data sets. Integration linkages clearly documented with risks and dependencies. With relevant supporting integration plans. Clear role designs and responsibilities with supporting access management to data and transactions.

SOW #	Title	Key Pillars	Scope	Assurance outcome
3	Transaction & Integrity – Financial Accuracy and Completeness	1. Finance 2. Retail 3. Legal & Compliance 4. Business Support	To ensure the financial accuracy / completeness of transactions and relevant controls and monitoring is in place. Review the reports that are planned or available to support financial transactions including reports that support the sub-ledgers and general ledger and production of financial statements-cash flows, Income Statement, Balance Sheet etc. Review and assess design of exception reports designed to support daily, weekly, month, quarterly and annual operations. Assess whether controls and reconciliations (Control Framework) built into the process to ensure relevant Management Review Controls can operate successfully.	SPMP ensures Financial Transactions are complete, accurate, supported and evidenced. With reporting and monitoring in place to identify and correct any identified issues, exception, anomalies etc.
4	Platform Security Resilience – Insider Threat	All pillars, key focus on 1. Security 2. Finance 3. Retail 4. Business Support 5. Inquiry	To ensure the platform can withstand insider threats - To validate that robust controls are in place to protect the platform from unauthorised access and DLP (Data Loss Prevention). Supported with the relevant training and awareness. Assess whether tooling is in place to identify (proactively and retrospectively), capture and report on insider threats and assess whether remediation processes are set in place to counter such instances. Review adequacy of MI and EWI in place to support the business processes reporting and management, including oversight/reporting at a senior level. Including a review of the following: • Continuous vulnerability Management • Audit Logging Management • Malware defences • Data Recovery • Penetration Testing • IT/DR Recovery. And identifying and understanding Policies, Procedures and training in place at POL and CISO input.	SPMP is accessing and designing preventative and monitoring measures to manage Insider threats. Control's must be fully documented and supported by KPI/KRIs. Supported with the relevant MI that is timely and accurate for management to take relevant actions to prevent or detect future threats.

SOW #	Title	Key Pillars	Scope	Assurance outcome
5	Platform Security Resilience – External Threat	All pillars, key focus on 1. Security 2. Finance 3. Retail 4. Business Support	To ensure the Network Infrastructure can withstand external threats. Adequate preventive and monitoring mechanisms are designed: • Assessment of network architecture, configuration, & security controls. • Evaluation of firewall configurations, intrusion detection/prevention systems, and network segmentation. • Review of network devices, such as routers, switches, and access points, for vulnerabilities and misconfigurations. Including a review of the following: • Continuous vulnerability Management • Audit Logging Management • Malware defences • Data Recovery • Penetration Testing • IT/DR Recovery. And identifying and understanding Policies, Procedures and training in place at POL and CISO input.	SPMP is accessing and designing preventative and monitoring measures to manage External cyber threats. Control's must be fully documented and supported by KPI/KRIs. Supported with the relevant MI that is timely and accurate for management to take relevant actions to prevent or detect future threats.
6	Defects and Risk Management	All pillars, key focus on 1. Software Delivery 2. Hyper Care 3. Business Support 4. Transaction Integrity 5. Security 6. Governance 7. Retail	To assess application and documentation of testing/defect methodologies across the end-to-end software delivery life cycle. To ensure appropriate ERM is applied in the assessment of defects (functionality, performance, Security, etc) and or acceptance of defects vs risk profiles in isolation and or in aggregate. Assess appropriate sign off and governance applied to testing and defects management. To ensure PEN's are managed, prioritised and addressed in accordance with good business practice and reviewed and approved with those in authority.	SPMP has applied testing in a consistent manner, with appropriate consideration to risks and key SME are involved in risk assessments and decision making. Clear evidence that defect management and PENs are well managed with robust controls, measures and align with good business practice, with the relevant approvals and oversight.
7	Software Delivery	All pillars, key focus on 1. Software Delivery 2. Hyper Care 3. Business Support 4. Transaction Integrity 5. Security 6. Governance 7. Retail	Review of software delivery processes / development life cycles processes and procedures. Assess application of good practices, process methods, testing eg UAT, defect management and compliance with the defined deliverables. Assure whether all activities clearly controlled and documented. Overlap - Controls around defect management will also feature as part of this review.	Clearly able to demonstrate throughout the Software delivery stages that good practice has been applied and supporting documentation / artefacts available to support decisions, conclusions and approaches adopted.

SOW #	Title	Key Pillars	Scope	Assurance outcome
8	Security (Account Management, User Access Control, Audit Logging) & User access (logical))	1. Software Delivery 2.Security 3.Retail 4.Business Support 5. Hyper Care 6. Transaction Integrity	To assess that adequate preventive and monitoring controls are designed over Access and Identity Management. To assess whether super users' profiles are commensurate with roles/profiles. Review whether all profiles accessing data (read only, edit, etc) are identified and controlled. Including a review of the following: • Review of IAM (Identity and Access Management) processes, including user account provisioning process, authentication, and access controls, Access control lists • Assessment of privileged access management (PAM) controls. • Evaluation of single sign-on (SSO) and multi-factor authentication (MFA) implementations. • Analysis of Access logs and audit trails • Automated tools or scripts used for scanning and assessing access configurations. And identifying and understand Policies, Procedures and training in place at POL and CISO input.	To assess whether the programme understands the technology landscape to pinpoint exhaustively points of access (PM. POL. Third parties, etc). SPMP user access is structured, defined, exhaustive and governed. And authentication is robust from a security perspective, including the Segregation of Duties (SoD).
9	Postmaster Support	1.Retail 2.Transaction Integrity 3. Business Support 4. Culture 5. Gating 6. Business Readiness	To assess whether processes and procedure, designed and documented to support PM transition to SPMP. Assess efficacy of PM Training/communication etc. Review whether issue judgments have been appropriately considered and actioned – HIJ, CIJ, Training. Assess whether hyper care is designed around PM.	Training and Detailed Procedures are in place to support Post master's both pre and post go-live. Hypercare arrangements and Business Support processes and procedures are fit for purpose to support PM in transition. Robust governess supported by adequate and appropriate EWI, KPI's and KRI's.
10	Data Privacy	1. Data 2. Security 3. Transaction Integrity	To review and assess whether Data Privacy principals are appropriately designed and embedded to protect Postmaster, POL, and other key sensitive data types. Assess adequacy of: • Data classification, encryption, and access controls. • Assessment of data retention policies and procedures. • Compliance with data protection regulations (e.g., GDPR, HIPAA, CCPA).	SPMP has designed and deployed Data Privacy principles that protect PM and POL, And other sensitive data. Appropriate and relevant restrictions and encryption are in place to support security and protection of data and ensure compliance to relevant data protection regulations.
11	Gating and Business Readiness	1. Governance 2. Business Support 3.Software Delivery 4. Retail, Security 5. Legal & Compliance 6. Gating	Assess whether Gating decisions are based on sound data and MI, and key SMEs input. Review the E2E gating process / methodology to ensure appropriate controls are in place to provide key decision and control points in the programme's delivery life cycle.	SPMP has a clear methodology and approach for gating and business readiness. With the relevant governance to ensure that key SMEs are involved in decision making and outcomes documented to evidence the decision-making process.

SOW #	Title	Key Pillars	Scope	Assurance outcome
12	Library of key controls – design, coverage, monitoring including efficacy of KRI, KPI, EWI etc.	1. Governance 2. CIJ 3. Security 4. Business Support 5. Transaction Integrity 6. Retail, 7. Data 8. Finance 9. A&CI	To review whether the design of key indicators/controls to ensure POL has adequate coverage on the E2E platform and sufficient early warnings designed to ensure no adverse impacts to PM or POL. Assess whether appropriate RACI and DOA (Delegation of Authority) in place to ensure timely visibility and decision making. Review whether a library of controls, with clear ownership, accountability and tracking exists.	POL governance is designed appropriately with adequate MI and escalation by design, to support and ensure an appropriate control environment.
13	CIJ / HIJ Conformance (Including Postmaster Detriment)	All pillars will be engaged throughout all reviews with a specific focus at point of "go live"	To assess that lessons from the past have neem embedded in SPMP design and clear outcomes and that mistakes and errors will not be repeated. This will involve a line-by-line review to access how issues from the past (CIJ & HIJ) have been or are being address by the programme and BAU Assurance.	SPMP can clearly demonstrate lessons have been learnt and all HIJ / CIJ observations have been addressed as part of design, build, test, and deployment. And that clear monitoring mechanics are in place contingent of the release strategy of SPMP.
14	Programme Planning and Release Management	1. Governance 2. Business Support 3. Software Delivery 4. Finance 5. Gating & Business Readiness 6. Legal & Compliance	To assess whether there is a robust Integrated Programme Plan along with a good release strategy to support the release and rollout of SPMP to branches. This will encompass: 1) Alignment of the Programme Planning with the Technology Delivery Roadmap. 2) Current status of the Programme Plan in relation to targets, timelines and budgets clearly defined. eg Backlog Management. 3) KPI's and related measures that demonstrate effectiveness of planning and how poor trends (early warnings) are addressed. 4) Review process, controls, methodology supporting planning and release. This will cover historic (eg lessons learnt) and planned (eg identified risks) to ensure effective and aligned with good practice. 5) Reporting, communication, and document controls effective. 6) Application of good practice application and management of Agile methodology. 7) Organisational clarity and defined R&R in this arena. 8) Integrated plan and milestone management/governance.	A robust integrated programme level plan exists combining the technology delivery roadmap, including clear documentation of assumptions, dependencies, and milestones. Also proving this has been tracked and regularly reported by PMO.

15	Vendor Management / 3rd Party Management	1.Security 2. Retail 3. Contract Management 4. Legal & Compliance 5. Business Support 6. Procurement	To assess and review the robustness of POL policy, process and governance applied to the selection, acceptance and controls established to obtain vendor / 3rd party support for the SPMP Programme. Review the adequacy of vendor management and performance related process and procedures. Review design and oversight mechanisms for 3rd parties.	There is clear evidence that the vendor selection process and compliance to policy has been applied and effectively managed. With the relevant up to date DOA applied to spends and approvals. Ensure robust vendor performance management and monitoring is in place.
SOW #	**Title**	**Key Pillars**	**Scope**	**Assurance outcome**
16	Software Delivery Life Cycle	1.Governance 2. Software Development 3. Security 4. Data 5. Retail 6. Business Support 7. Transaction Integrity	The review will focus on: • Performing sample reviews on key process and procedures eg JIRA, EPIC and User stories, Coding Standards, Tooling, test scripts etc. Assessing application of standards, practices and quality frameworks. • Assess whether robust policies and procedures are in place to manage 'change control, to ensure alignment with business requirements but also delivery of BC objectives and outcomes. • Review whether appropriate Governance (incl KPI/KRI) and oversight exists. • Review how PMO understand and assist in the identification of risks, issues, assumptions, and dependencies. • Assess how the Programme Team drive continuous improvement.	To ensure that good practice has been applied across Governance Gates and protects integrity of the code For environment change requests a formal and established gating process and procedure are embedded. Detailed evidence retained to ensure that the correct level of attention has been applied to ensure the desired outcomes of the SPMP platform delivery/BC. Also, identification of any potential deviations and how change management principles have been applied managed correctly.
17	Enterprise Assets Logging Enterprise Asset Software	1.Security	To perform a deep-dive technical assessment into available system logs relating to security and incident monitoring. The scope of the review will focus on: • Assessing the processes and data sources available that relate to the logging functionality for security events and sensitive transactions. e.g. Review logging functionality for security events, review the logging functionality for sensitive transactions • Review the process designed to analyse the logs and address exceptions • Review the process designed to respond to suspicious activity discovered in the logs (manual, automated), and any incident response and handling. Management of PEN's including planning, remediation and closure.	To ensure that rigorous processes and controls are in place and followed to support enterprise assets logging and software. And detailed evidence exists to demonstrate the logging functionality for security events and sensitive transactions are robust and in line with good practice and required policies. With relevant processes to support monitoring, reporting and taking preventive action.

SOW #	Title	Key Pillars	Scope	Assurance outcome
18	Network Infrastructure Network Monitoring	1. Security 2. Retail 3. Transaction Integrity	Assessment of network architecture, configuration, and security controls. Evaluation of firewall configurations, intrusion detection/prevention systems, and network segmentation. Review of network devices, such as routers, switches, and access points, for vulnerabilities and misconfigurations. Web & Email Browser Protection / Cyber Security. Assess whether good practice (eg ISO) have been applied to security architecture, vulnerabilities, monitoring for change and configuration controls. Review will also focus on the network monitoring controls to ensure countermeasures are deployed to prevent intrusions and attacks to the network. The review will also encompass: 1. Configuration management system: to track and manage configurations of network devices 2. Baseline configurations: establishing and maintaining secure baseline configurations for different types of network devices to reduce vulnerabilities 3. Change management processes: to ensure that any changes to network decide configurations are documented, reviewed, and authorised 4. Vulnerability scanning tools 5. Patch management 6. Network segmentation 7. Logging and monitoring systems 8. Incident response plan 9. Employee training 10. Regular audit and reviews.	Clear evidence of robust controls & processes, with supporting evidence / artefacts, confirming the network infrastructure and measures are managed in accordance with good practice and defined POL / Regulatory requirements.

SOW #	Title	Key Pillars	Scope	Assurance outcome
19	Application Software Security	1. Security 2. Software Delivery 3. Retail 4. Data 5. Inquiry	Review of Application Security to ensure that relevant tools have been deployed and monitoring activities are in place to prevent and detect intrusions and attacks. Assessment of application development practices, including secure coding standards and vulnerability management. Review of application architecture, design, and access controls. Penetration testing and vulnerability assessments of web applications, mobile apps, and other software systems. The review will also encompass: 1. Static Application Security testing (SAST) 2. Dynamic application security testing (DAST) 3. Security training for developers 4. Secure development frameworks 5. Incident response plan for application security 6. Dependency scanning.	Programme can demonstrate that there are robust processes and procedures in place to demonstrate practices and testing to prevent and detect security risks at an application level.
20	People & Culture	All pillars, key focus on 1 Governance 2. Legal & Compliance 3. A&CI 4. Contract Management 5. Culture 6. CIJ 7. Business Support 8. Retail 9. Inquiry	Review will focus on SPMP Roles and include validation: To assess whether the SPMP programme has adopted and embedded the appropriate process and procedures in place to embed the right culture and people into the organisation aligned with achievement of strategic and operational objectives. Assess how key cultural and people thematic from CIJ and HIJ are applied and sustained. To review the establish the effectiveness of WoW and how managed across the programme. Assess how TOM for business support and BAU Retail Operations embed the right cultural and people values aligned with the issue judgements. Review the training in place upon entering the POL and the subsequent training that supports employees understand and adhere to the culture aspects of POL. Assess how new roles and specs are created to ensure alignment with business purpose and objectives. Set KPI's / measures in place to identify success in this area (eg attrition) and how poor trends are addressed.	Clear evidence available demonstrating good practice covering all elements of people and culture across the programme. This will include: 1) Records of training covering onboarding new staff and ongoing training supporting identified training needs 2) Effective comms to support staff and advise of current / new initiatives in this area of the business 3) Measures of effectiveness of WoW culture 4) How lessons learnt have been addressed 5) KPI's / Measures in place to identify poor trends (eg attrition) and how they are resolved / mitigated 6) Clear reporting to the senior team on status, risks, issue resolution and planning.

SOW #	Title	Key Pillars	Scope	Assurance outcome
21	Incident Response and Management - Penetration Testing	1. Software Delivery 2. Security 3. Retail 4. Legal & Compliance 5. Data 6. Inquiry	To ensure that Penetration Testing is fully controlled in alignment with good (business / Regulatory / ISO) practice. Scope of this review will also look at: • intelligence gathering eg network and domain names, mails server to see how targets are focussed and vulnerabilities identified. • Process and controls around incident management including but not limited to: • Incident response plans, procedures, and capabilities. • Backup and recovery processes, including testing and validation. • Incident detection and response tools, processes, and training.	To have obtained details of established processes and controls around the E2E penetration testing activity.
22	Business & IT Controls Library	1.Governance 2. Software Delivery	Assess Business Controls/IT that have been documented to date for programme/POL. Assess how control coverage and design is adequate and covers the risk landscape of SPMP/POL. Assess the applications of these controls and identify and gaps of application/remediation. Scope of this review will also look at • Risk library (business and IT) • Control library (business and IT) • RACI by process and controls • DOA • SoD and Access Management • Security and Integrity • MI/Reporting and Governance, including REN and PENs.	POL is able to monitor and measure the efficacy of it control environment vs the release profile of SPMP.

SOW #	Title	Key Pillars	Scope	Assurance outcome
23	Governance	All Pillars	Review the Governance arrangements within SPMP to ensure robust practices exist for: • Progress Tracking and Reporting – tracking and reporting of progress including the programme financials is in place on the programme; status reporting takes place to ensure that progress is being tracked and reported on the programme. Tracking, monitoring SPMP progress • Monitoring of KRI/EWI • Sufficient objectivity is in place to constructively challenge SPMP direction, risk assessments and outcomes. • Change management process and practices • Monitoring of BC and delivery of BR • Oversight of issue judgements • PM protection • Efficacy of reporting data sets with key business and SME input • Decision making and risk assessments • Planning and Dependency Management • Programme Structures - a RACI matrix is defined and in place for the programme and roles, responsibilities and accountabilities have been clearly defined and key roles on the programme have been filled. • Communications and Stakeholder Management – stakeholder mapping and communications plan for the programme is defined; lower-level communications plans outlining the timing of activities and responsible individuals has been defined for the programme. • Resource Management – there is a resource plan defined for the programme; ensure that the plan is maintained, and regularly reviewed and updated • Risk acceptances, inputs and continuous monitoring.	A robust governance approach in place to ensure successful delivery of SPMP in line with BC and BR.
24	Integration strategy (To POL strategies and wider systems)	1. Software Delivery 2. Data 3. Legal & regulatory 4. Contract Management	Review approach to systems integrated with the new NBIT platform to ensure they are/will be integrated and transferring, providing information accurately and timely between different systems. Review and understand what MI/reports and KPI's are in place to manage and monitor transference of data between systems, to ensure completeness, accuracy, and timeliness of transfer. Review whether sufficient and relevant integration testing has been carried out and signed off as part of the stage gating process by relevant and authorised individuals.	Evidence of a robust integration Strategy with other systems (SWIFT, Banking apps) Master data being relied upon by the programme is accurate and there are no inaccuracies in product set up or mapping. Ie no risk that results in incorrect postings to downstream systems. Systems integrated with the SPMP platform are providing accurate information and supporting evidence (controls/measures) are in place Accurate MI/KPI/Reporting available and evidence of effective action taken to address issues/poor trends. Evidence of testing conducted and completed with supporting processes and best practices controls Evidence to demonstrate that the key stakeholders have been engaged as part of the sign off / gating process.

SOW #	Title	Key Pillars	Scope	Assurance outcome
25	Legal Risk	1. Security 2. Legal & Regulatory	Review the Legal Risk Framework to evaluate and assess how: 1) Sources of legal risk are identified, e.g. contracts, regulatory, structural changes, and compliance. 2) Risks are defined vis a vis risks vs issues vs potential risks and potential issues. 3) Risks processes and controls to ensure risks are appropriately identified, managed and monitored. 4) RACI and DoA for management and assessment of Legal risk is appropriate and understood. 4) Monitoring and KPI - Aligned with high and low risk legal issues with appropriate planning to support. 5) Defined controls and measures aligned with HIJ / CIJ, and lessons learnt. 6) Alignment is assured with Programme Deliverables and Gating / No Go decision making.	Clearly defined processes with supporting evidence to demonstrate the controls and management of legal risks.
26	Retail Readiness and Support to Post Masters	Retail Business Support / Hypercare	The purpose of the review is to ensure the SPMP programme can demonstrate robust processes and procedures, which validate the retail readiness to receive the new platform from a Postmaster lens (PM). • Retail PM readiness plans – coverage and conformance with principles laid out within issue judgements. • PM Support and Training. • PM comms/engagement plans. • BSC Readiness – detailed procedure manuals etc. • Hypercare Arrangements. • PM Hardware and Commissioning. • Communication to PM's – clarity, approach and impact. • Role of BA and AM / RACI. • Transferring and cut off procedures from Horizon to SPMP. • PM routes to escalation and POL resolution SLA, and approach. • Approach and role of A&CI and Retail Assurance teams. • Plans for resourcing to ensure delivery. • Governance, KPI and Risk Management. • Adequacy and effectiveness of early warning indicators, with a key focus on PM wellbeing (CIJ). • Culture -Has PoL/Retail identified the right and appropriate mechanism and triggers to capture culture.	To have ensured that all elements of the Retail Readiness process is effectively Managed and providing the best level of control and support to Post Masters as part of the programme delivery requirements. Evidence obtained to demonstrate planning accuracy, efficiency in stock control, delivery planning, product verification, KPI's monitored to ensure poor trends/performance addressed, swap out and post-delivery support. Evidence of financial controls/planning and alignment with the Programme Plan will also have been validated.

SOW #	Title	Key Pillars	Scope	Assurance outcome
27	Cloud Security	Security	• Assessment of cloud infrastructure configurations (e.g., AWS, Azure, GCP). • Review of cloud service provider (CSP) security controls and shared responsibility models. • Evaluation of cloud identity and access management, data encryption, and compliance posture.	Ensured that controls, processes, and measures managing the cloud infrastructure, CSP security controls and identity and access management are in place and align with good business practice Ie ISO 27001.
28	End Point Security	Security	• Assessment of endpoint protection solutions (e.g., antivirus, endpoint detection and response). • Review of endpoint configuration management and patch management practices. • Evaluation of mobile device management (MDM) and bring-your-own-device (BYOD) policies.	Ensured that robust controls, processes, and effective measures are in place to manage endpoint protection, configuration, patch management and mobile device management. ISO 27001 / 27002.
29	Compliance & Regulatory Requirements / Frameworks	Security	• Assessment of IT controls against relevant regulatory requirements and industry standards (e.g., ISO 27001, NIST Cybersecurity Framework). • Review of compliance with specific regulations (e.g., PCI DSS, HIPAA, GDPR).	Validated, with supporting evidence, that all the programme IT controls are in compliance with POL and regulatory requirements. (e.g., PCI DSS, HIPAA, GDPR). The application and management of this being aligned to good business practice Ie ISO 27001.
30	Security Risk Management *Potential to merge with SOW 24	Security	• Evaluation of risk assessment methodologies and risk management processes. • Review of risk treatment plans and mitigation strategies. • Assessment of risk monitoring and reporting mechanisms.	Ensured the E2E Risk Management process is robust and followed in line with defined controls & processes. Evidence / artefacts seen to confirm good practice supporting risk assessment methodology, risk treatment / mitigation and effective monitoring. Good industry practice being aligned with ISO27001.
31	Security Operations (Organisation)	Security	The scope of Security Operations will be to look at the designed or to be designed Security Organisation (TOM) and assess: • Evaluation of security operations centre (SOC) processes and capabilities. • Review of security monitoring and incident detection tools. • Assessment of security incident response workflows and procedures.	Ensured that robust and defined Organisational Design including controls and processes are in place and followed to manage the security operations centre. Validated, with supporting evidence, the effectiveness of security monitoring / incident detection and response controls. This all being aligned with POL, regulatory requirements and good business practice Ie ISO 27001.
32	Disaster Recovery and Business Continuity	All Pillars	Review to ensure that POL standards are adhered to for Disaster Recovery and Business Continuity. Review to include assessment of: • measures of effectiveness and how controls are tested and enhanced to align with pre and post (Final Platform) deliverables. • DR and BC RACI. • Approach to integrated testing, including approach to cyber threats • Roll back process and procedures	To ensure robust DR and Business Continuity plan is in place with supporting processes. Detailed evidence of how the plans are tested to ensure effectiveness and alignment with the platform during release phases and current planning(preparation) for final release. Full ownership and RACI to support this model has been defined. All planning aligned with good business practice and POL / Regulatory requirements

SOW #	Title	Key Pillars	Scope	Assurance outcome
33	Finance & Cost Model	1. Governance 2. Finance 3. Inquiry	To review the Financial Cost modelling of the SPMP programme to ensure that costs being incurred are accounted for are completely and accurate. Including the accounting principles being followed. Review the linkage of the cost model to the Business Case and Business Requirements. And how changes in the Business Case and Business Requirements are being reflected into the Finance Cost Model. Review the processes in place to monitor and manage Actuals to Budget/Forecast. How exceptions and deviations are being escalated and addressed.	Ensure that there are robust processes and procedures in place to capture and appropriately account for SPMP cost, including the monitoring and reporting against budgets /forecast. Ensure alignment with BC and BR.
34	Business Case and Benefit Realisation Assurance	1.Governance	The scope of the Business Case and Benefit Realisation review will consider: a Modelling for business case and benefit realisation is sufficiently robust and appropriate b Sufficient to support funding draw downs c Captures impacts of risks, issues and assurance reviews/outcomes d BC and BR change management process is robust.	Ensure that there is a robust model in place for the Business Case and the linkage into Business Requirements and delivery. Provide an opinion on the Cost, Benefits realisation model and assumptions. Provide opinion on the monitoring and reporting mechanisms of the Business Case and change management.

POST OFFICE

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

3.4

Title:	Internal Audit Report	**Meeting Date:**	21st May 2024
Author:	Johann Appel – Director of Internal Audit & Risk Management	**Sponsor:**	Kathryn Sherratt – Interim CFO

Input Sought: Noting

The Committee is asked to:

i. Note the progress being made with delivery of the internal audit programme and completion of audit actions.

Previous Governance Oversight

RCC of 7 May 2024.

Executive Summary

Following are the key messages from this report:

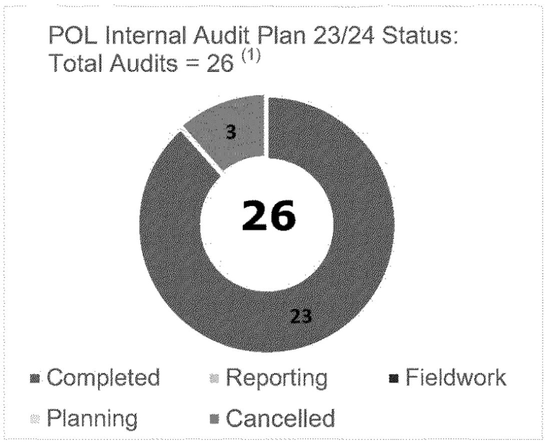
- **Progress with Internal Audit Programme:** We have now completed the 2023/24 internal audit programme. Six audits were completed during this reporting period:
    - Financial Services Conduct Risk Management – Needs Improvement
    - International Money Transfer - Needs Improvement
    - ATM Link Scheme Assurance - Satisfactory
    - Copper Stop Sell Programme – Significant Delivery Risk
    - Pin Entry Device Replacement Programme – Significant Delivery Risk
    - Management of Post-GLO Improvements – Needs Improvement
- **Progress with Audit Actions:** Completion of audit actions is progressing steadily. As of 13 May, there were 22 actions overdue, 14 of which were older than 60 days.

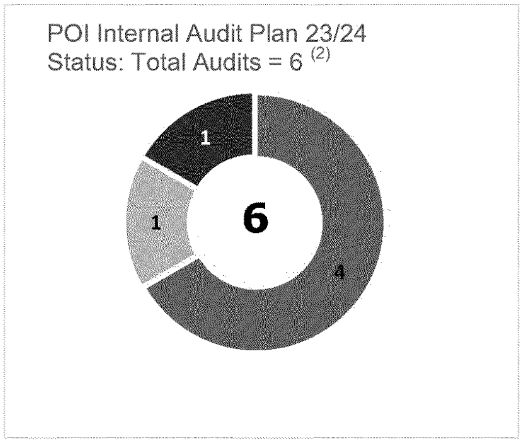
3.4

Report

Progress against plan for 2023/24

1. We have completed six POL audits since the March ARC.
2. The final status of the 2023/24 plan is as follows:





[1] Target number of reviews based on revised plan for 2023/24 approved by ARC in Sept 23 is 26 (20 Internal control reviews & 6 change assurance reviews). Details of the audit plan can be found in Appendix 1.

[2] POI ARC approved baseline plan for 2023/24.

3. Progress against the 2024/25 plan will be reported from July.

Internal Audit reviews completed

4. The following POL audits have been completed since the March ARC meeting:

	Audit Title	**Report Rating**
1	Financial Services Conduct Risk Management	Needs Improvement
2	International Money Transfer	Needs Improvement
3	ATM Link Scheme Assurance	Satisfactory
4	Copper Stop Sell Programme	Significant Delivery Risk
5	Pin Entry Device Replacement Programme	Significant Delivery Risk
6	Management of Post-GLO Improvements	Needs Improvement

5. Key risk and control themes from these reviews are:

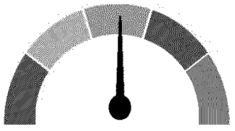
- POL does not separately identify subsidiary or appointed representative risk in SNow and, as such, these areas have no assigned risk owner.
- MoneyGram and Western Union products are generally well managed, although there is a need to improve risk management and to validate management information received from product providers for revenue calculations and performance KPIs.
- The Copper Stop Sell programme experienced high failure rates due largely to a recognised gap in Postmaster communications across the programme portfolio,

supplier communication issues, and site-specific challenges due to prior site assessments not being funded.

- There is a lack of coordinated communication with postmasters and a single source of contact details for postmasters when rolling out changes to the network.
- Whilst good progress continuous to be made with Post-GLO improvements, there is a need to improve the tracking of actions and deliverables.

6. Below are summaries of the adversely rated reports.

7. **Copper Stop Sell Programme** (Ref.2023/24-21)



Significant Delivery Risk

Audit actions:

P1	4
P2	4
P3	-
Total	8

Sponsor: *Chris Brockelsby (Paula Jenner)*

Reading Room attachment 2

BT Openreach are replacing the existing copper Asymmetric Digital Subscriber Lines (ADSL) with a new fibre infrastructure, ending the sale and support of copper products where fibre alternatives were available by September 2023, and completely withdrawing copper services by December 2025. The Copper Stop Sell programme aims to mitigate impact on the network of the loss of copper ADSL, address the existing router estate running out of manufacturer support in May 2025, and expand LAN Port availability to meet future demand.

The objective of this review was to assess the effectiveness of governance and control of the programme, and management of delivery risk.

Whilst some areas for improvement have been identified, the programme is generally well managed in line with the Change Excellence Framework (CSF), and it has shown resilience and innovation to meet external challenges. However, **failed install rates remain high**, due largely to a recognised **gap in Postmaster communications** across the programme portfolio, supplier communication issues, and site-specific challenges due to prior site assessments not being funded.

At date of reporting **BT Openreach cannot provide technical solutions for 800 branches** (down from 3000 at date of review). Use of traditional ADSL lines can be extended, but there is a hard cut-off to migrate these branches before NBIT roll out. This highlights the dependency on BT Openreach, for whom this is a large, complex programme. Based on our findings we have rated this report "**Significant Delivery Risk**".

Management Comment by Paula Jenner, Core Products and Platforms Director

"Whilst I agree with the recommendations and agreed actions it should be recognised that the transformation being undertaken by BT is a major and complex programme of work with is inherent with its own challenges and changes to previously communicated schedules. Post Office are dependent on BT's wider programme to enable successful delivery of the Copper Stop project, and this coupled with the complexity in the branch landscape and the numbers of vendors involved in delivering means there is more risk of a domino effect if there are failures in each of the transformation activities.

Area 1:I note the mention of a central database of CAD drawings for each branch are already available within the business. Given the Retail involvement in the programme and the representation on the Steering Group I'm concerned this has only just come to light. The data within this database would have been invaluable to the project during the planning stages and may have prevented some of the failures to date. It would be prudent to ensure the existence of this database is common knowledge within the Change Portfolio.

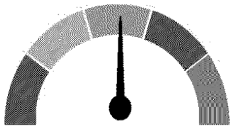
Area 2:While a formal Contingency plans and a clear critical path have rightly been identified as priority actions, given the complex nature of the programme it should be understood there is likely be a level of uncertainty regarding milestone dates within the critical path. It is also worth noting the agile way in which the project team have been operating in conjunction with our Vendors. The project team are focused on meeting the Dec

2025 date and are agile in the way they respond to changes in plans to ensure we meet that date. The significant decrease in numbers of branches without a solution is further evidence of Post Office's reliance on the BT Transformation programme and how quickly the risks and plans can change.

Area 3: Postmaster communications – I am in complete agreement with the assessment documented. It is well recognised across the project delivery landscape that the absence of a centralised team for branch communications along with robust and reliant contact information for our Branches is a challenge for any project that touch the branch estate. Postmaster representation – Although I agree with the findings it should be noted that some of the current project team roles are filled by previous postmasters.

As a final note - I would like to commend the PM, project resource and BAU Technology team on their input and management to date on what has been and continues to be a challenging project for Post Office. Regardless of the importance of this project to continued trading; it has been difficult to secure the realistic funding required and therefore the project approach has had to take this into account during resourcing and planning. The agility and tenacity of the team has enabled the delivery so far."

8. **Pin Entry Device (PED) Replacement Programme** (Ref.2023/24-24)



Significant Delivery Risk

Audit actions:

P1	5
P2	4
P3	1
Total	10

Sponsor: *Chris Brockelsby (Greg Hunt)*

Reading Room attachment 3

The PIN Entry Device (PED) enables the processing of credit and debit card payments either through keying a Personal Identification Number (PIN) or using Near Field Communication (NFC) to complete a contactless transaction. The IPP350 terminals reached their end-of-life in April 2021 and will no longer be supported or repaired by Worldline post December 2023. Furthermore, the PCI PTS (Payment Card Industry Pin Transaction Security) certification is no longer compliant with PCI requirements after April 2026. The programme aims to address both of these challenges by replacing these devices.

A number of common themes have been identified with the Copper Stop Sell programme which IA reviewed in February 2024, many of which are outside the control of the programme. In particular a need for a more coordinated approach to communicating with postmasters, drawing on a single, complete and up to date source of postmaster contact details which is compliant with General Data Protection Regulation (GDPR) requirements. However, it should be noted that steps have been taken during these reviews to start to put in place a central function, and a 'single source of truth' database.

Overall, project management and governance were reasonably robust. However, greater focus on lessons learned and contingency planning is required. Reporting of PED replacement installations in branches through the pilot phase should also be strengthened, and there is a need for greater clarity on counter rationalisation, in order to effectively deliver procurement and rollout planning.

The programme has been delayed by three months while Worldline attain PCI certification on the new PED. This compounds other significant risks to delivery, including the dependency on, and lack of visibility of, the counter rationalisation programme, the absence of a rollout plan, and the dependency on approval of a yet to be submitted change request in order to agree contingency funding. These collectively present major delivery risk, and at the date of our review the programme had rated itself red to reflect this. However, there is clear evidence of steps being taken to mitigate these risks and on this bases we have rated this report "Significant Delivery Risk" moving towards "Some Delivery Risk".

Management Comment provided by Greg Hunt, Head of IT Service – Branch Products and Platforms

Whilst I recognise and agree with the findings within this report, it's worth pointing out that a number of the key priority findings and risks fall outside of the PED programme's scope to resolve.

Specifically, the P1 findings in relation to the dependency on the counter rationalisation; the finding with regards to no central function for coordination of postmaster engagement on projects and programmes and there being no reliable single source of postmaster contact details.

For the other findings that have been highlighted during the audit - the programme has either resolved the finding, or there's a clear plan in place to address.

Update on Horizon Privileged Access Management

9. Following a management request in 2023, Deloitte have completed a review of Privileged Access Management (PAM) in Horizon. The full report is available in the reading room (appendix 8).

10. Due to a lack of cooperation provided to the fieldwork team by Fujitsu, who are responsible for managing privileged access to key components of HNG-A, several intended scope elements could not be completed and the review therefore focused on POL operated controls only. As the auditors were unable to test access controls operated by Fujitsu, Deloitte could not reach an opinion and therefore have not rated this report

11. Five key areas were highlighted for improvement, which are:
    (a) A lack of oversight and governance by POL over controls performed by third parties;
    (b) A lack of up-to-date policies and procedures;
    (c) Ineffective branch-level privileged access management;
    (d) Lack of robust user access review processes; and
    (e) An excessive number of Global users with privileged access to account management and transactional activities across all branches.

12. A service organisation controls (SOC) (ISAE 3402) review for Fujitsu is currently being performed by EY, who are expected to finalise their report by August 2024.

13. We propose that Internal Audit review the scope and results of the SOC review to determine if this provides adequate coverage and assurance over PAM. In addition we propose a follow-up audit to validate that the findings from Deloitte's review have been addressed.

Internal Audit reviews in progress

14. The following audits from the 2024/25 programme are in progress or being planned for delivery at the July ARC:

	Review	Sponsor	Status
1	Incident management and Breach Reporting	Chris Brocklesby	Fieldwork
2	SPM Security Phase 1 (Data Breach Root Cause)	Chris Brocklesby	Fieldwork
3	Support & Maintenance of Back-Office Systems	Chris Brocklesby	Planning
4	2023/24 STIP Metrics	Karen McEwan	Planning

3.4

Changes to Internal Audit programme for 2024/25

15. Following a recent data breach incident, management requested that Internal Audit perform an investigation to establish the root cause of the incident. This work will be done in two phases as follows:

    - A 'lessons to learn' review of the Incident Management and Breach Reporting process to establish why the breach was not escalated and reported in a timely manner. This is an addition to the 2024/25 plan;
    - A root cause analysis to understand how and why a third party outside of the UK had access to customer data. This work will be done as part of the scheduled SPM Security review, which has now been brought forward.

16. DBT have requested that IA provide assurance over the design of the POL Process Review (PPR) redress scheme. This assurance is a condition for DBT to release the funding.

17. Management have requested that IA validate the 2023/24 STIP bonus metrics outturn.

18. The ARC Chair have requested that IA provide assurance over the completion of actions from a recent speak-up investigation.

Status of Audit Actions

19. There are currently 22 actions overdue, 14 of which are older than 60 days.

20. The movement and ageing of audit actions are shown in the table below (status as of 13 May 2024).

Audit Action Status (POL):		**Ageing:**	
Open actions at last ARC	63	Open (not yet due)	55
Less: Actions closed in period	8	Overdue (<60 days)	8
Add: New actions in period	22	Overdue (>60 days)	14
Total open actions	**77**	Total open actions	**77**

21. Breakdown of the actions that are overdue for more than 60 days:

Audit / Area	**No. of actions > 60 days**
Payroll	2
IT Control Framework	2
Contractor Hiring	8
Cyber Resilience [N1]	1
Horizon Change Management	1
Total	**14**

[N1] One action from the Cyber Resilience review has been overdue for 13 months (key security controls and tools to mitigate malware attacks). This action comprised multiple activities, most of which have been completed (including implementing Multi-Factor Authentication). However, the Branch Security Risk Assessment has not yet been finalised, although we understand a draft assessment has been created.

POI Audit Programme

22. The table below shows the status of the 2023/24 POI audit programme, which is reported to the POI ARC:

	Proposed Review	ARC reporting	Status / Rating
1	Webhelp Transition Plan – Ph 1	Jan-24	Unrated
2	Webhelp Transition Plan – Ph 2	Apr-24	Unrated
3	Third Party Oversight	Nov-23	Needs Improvement
4	Cyber Security	Apr-24	Fieldwork
5	Risk Management	Apr-24	Reporting
6	Fin Ops Controls	Jan-24	Needs Improvement
7	Pricing Controls		Delayed to 24/25 Plan
8	Demonstrating Independence Follow-up (focused)		Delayed to 24/25 Plan

Appendices[1]

Appendix 1: Internal Audit Programme for 2023/24
Appendix 2: Internal Audit Report – Copper Stop Sell Programme
Appendix 3: Internal Audit Report – PED Replacement Programme
Appendix 4: Internal Audit Report – ATM Link Scheme Assurance
Appendix 5: Internal Audit Report – Management of Post-GLO Improvements
Appendix 6: Internal Audit Report – International Money Transfers
Appendix 6: Internal Audit Report – Conduct Risk Management
Appendix 8: Deloitte Report – Horizon Privileged Access Management

[1] Appendices are accessible in the CoSec 'Reading Room'

Appendix 1 2023/24 IA Plan – ARC approved March 2023, refreshed September 2023

No.	Title/Subject	Sponsor	Resource	Comments (changes tracked in red)	Timing	Status / Rating
Internal Control Reviews						
1	ATM LINK scheme assurance	Owen Woodley	In-house	Original plan	March 24	Satisfactory
2	3rd Party Revenue Data Validation - NFS	Al Cameron	In-house	Carried forward from 2022/23	April 23	Needs Improvement
3	3rd Party Revenue Data Validation – ATM revenue	Al Cameron	In-house	Carried forward from 2022/23	April 23	Satisfactory
4	Financial Reporting Controls	Al Cameron	Co-source	Original plan	June 23	Needs Improvement
5	Postmaster On-boarding Financial Approvals Process	Martin Roberts	Co-source	Original plan with scope change	July 23	Needs Significant Improvement
6	Stamp Stock Controls	Martin Roberts	Co-source	Original plan	Sept 23	Unsatisfactory
7	Management of Post-GLO Improvements (IDG 2.0)	Nick Read	Co-source	Original plan	Oct 23	Needs Improvement
8	Overturned Convictions (Phase 1)	Simon Recaldin	Co-source	Original plan	July 23	Unrated Report
9	Overturned Convictions (Phase 2)	Simon Recaldin	Co-source	Original plan	Jan 24	Cancelled
10	HSS	Simon Recaldin	Co-source	Original plan	June 23	Needs Improvement
11	Postmaster Redress (Suspension Remuneration Review)	Martin Roberts	Co-source	Original plan	Dec 23	Needs Improvement
12	FS Conduct Management	Owen Woodley	Co-source	Original plan	Oct 23	Needs Improvement
13	Sales (International Money Transfer)	Owen Woodley	Co-source	Original plan	March 24	Needs Improvement
14	Contractor Hiring Process	Ian Rudkin	Co-source	Original plan	July 23	Needs Significant Improvement
15	HIJ Phase 3	Jeff Smyth	Co-source	Original plan	Dec 23	Low Delivery Risk
16	Cyber Security Maturity Assessment	Zdravko Mladenov	Co-source	Original plan	Oct 23	Unrated Report
17	Cloud Security	Zdravko Mladenov	Co-source	Original plan	June 23	Needs Significant Improvement
18	IT Vendor Risk Management	Zdravko Mladenov	Co-source	Original plan	Q2	Needs Improvement
19	Validation of 2022/23 Bonus Metrics	Ian Rudkin	In-house	Addition to plan, management request	Q1	Unrated Report
20	Inquiry Programme (Disclosure Processes)	Diane Wills	In-house	Addition to plan, management request	Nov 23	Cancelled
Change Assurance Reviews						
1	Data Centre Fortification	Jeff Smyth	Co-source	Original plan	June	Significant Delivery Risk
2	Application Modernisation	Jeff Smyth	Co-source	Original plan	May	Some Delivery Risk
3	PCI Compliance	Jeff Smyth	Co-source	Original plan	Oct	Significant Delivery Risk
4	Copper Stop Sell Programme	Chris Brocklesby	Co-source	Addition to plan, management request	Feb	Significant Delivery Risk
5	Pin Entry Device (PED) Replacement Programme	Chris Brocklesby	Co-source	Addition to plan, management request	March	Significant Delivery Risk
6	SPM Programme Placeholder	Chris Brocklesby	Co-source	Original plan	Q3	Delayed to 2024/25
7	SPM Programme Placeholder	Chris Brocklesby	Co-source	Original plan	Q3	Delayed to 2024/25
8	SPM Programme Placeholder	Chris Brocklesby	Co-source	Original plan	Q4	Cancelled

3.4

POST OFFICE

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Title:	Data Governance Update	**Meeting Date:**	21st May 2024
Author:	Chris Russell, Interim Data Management Director	**Sponsor:**	Tim McInnes, Strategy & Transformation Director

Input Sought: Noting

The Committee is asked to note:

- The status and progress being made on improving the data maturity profile of POL.
- The next steps to drive a sustainable and robust approach towards data management.

Executive Summary

Based on feedback from the ARC in 2023, the Interim Data Management Director has been re-assessing options available to bring forward the data maturity targets that were initially set at achieving IRRELEVANT by 2027 and thereby bringing the data management risk within appetite sooner. (Please refer to **Appendix 1** for maturity levels).

The current status is as follows:

- All Functions with exception of RU and Inquiry are expected to achieve IRRELEVANT maturity by July 2024. Given the current pressures within RU and Inquiry, we have agreed a revised maturity timeline of September 2024, and additional Group Data Management support is being provided to ensure this timeline is met and or brought forward.
- To assess how the timelines for IRRELEVANT maturity can be brought forward from August 2027, a pilot scheme is being stood up which will be taking three areas of the business (SPMP/FDP and one TBC business area) to IRRELEVANT maturity by the Q4 24/25.
- The key risks associated with reaching IRRELEVANT maturity by 2027 or earlier are.
    - time taken to reduce the risk score to be within risk appetite.
    - The impact of remediation required within the business weighed up against business as usual.
    - Regulatory, legal, contractual, and reputational impact of any non-compliance with obligations.
    - A lack of conformity across POL in key definitions of data terminology leading to inconsistency within different programmes of work.
    - Further work that may need to be added to the programme because of recommendations from the ongoing statutory Inquiry.
    - Availability of additional resourcing (during 2025-26) during the latter stages of Levels IRRELEVANT to ensure the integrity of the data captured within the Data Governance Framework is not compromised.
- We are now adopting a revised approach to assess the core components of data maturity and the timelines associated with these, such as:
    - Criticality of Data Sets – working with the business and Data SME's across POL the pilot will define 'Critical Data Set' and then focus maturity activities on those sets.
    - Impact on all POL's business given that the activities are resource intensive.
    - Considering the activities set out in the Maturity Framework (See Appendix 2) and revising the framework accordingly to be shared with ARC at the September 2024 meeting.

- Managing POLs risk exposure.

Whilst we have not prepared a detailed revised timeline, we believe we have created the right approach based on risk, critical data sets and burden on the business. During the proposed pilot scheme, we will keep ARC updated on progress and issues arising and on conclusion of the pilot scheme present the more detailed timelines to ARC.

Report

1. The Data Management Team has been in operation since 2021 with an initial focus of baselining a programme of work to deliver a sustainable, scalable, and robust level of maturity for data governance across POL. At the heart of this work was three core principles:
   a. All data sets across POL identified and assigned Data Owners.

   b. To support and facilitate data governance related objectives borne out of HIJ Remediation Actions.

   c. In addition, the quality of the data assessed and where the quality of the data is found to be low then enhancements to that data will need to be made.

2. Work on delivering enhanced data governance maturity commenced in March 2023 with agreement from ARC to target IRRELEVANT maturity across POL (**see Appendix 2**). Data Sponsors and Deputy Data Sponsors were assigned and briefed on POL's aim to deliver a satisfactory level of maturity. At recent RCC meetings members have been briefed on progress as POL moves towards the first milestone of Level 2 compliance.

3. Key to ongoing activities has been the identification of what progress can be made with current funding levels and we believe that 13 out of 14 activities towards IRRELEVANT can be progressed without any immediate additional funding for the Data Management Team **(see Appendix 3)**. However, this will be burdensome across POL specifically around the identification of critical data sets, the collation of metadata for data cataloguing and data quality reviews. Whilst this is the case it is noted that all business areas are required to maintain a robust control environment of which data is an integral part.

4. For the long-term sustainability of IRRELEVANT maturity POL will need to consider investment for the automation of data cataloguing and quality. Any additional investment required will be scoped out and presented over the next 12 months with additional funding being sought in the FY25/26 plans. In the interim the Data Governance Team are in discussions across POL and key data areas to assess where additional resources may be shared.

5. The Pilot scheme mentioned earlier will be targeted in key areas to POL and determined by the level off associated risk and criticality of data sets. Thus, the proposal is to include:

   a. **SPMP:** Given wide internal and external scrutiny on SPMP there is a clear need to progress data governance workstreams to ensure robustness and credibility of NBIT. This will be a critical input into building Postmasters' trust in the new system.

   b. **Future Data Platform (FDP):** Including FDP in the pilot will be beneficial given the criticality of the datasets sitting within this platform. In addition, this will help reduce the risk of implementation inconsistencies in key areas such as data cataloguing and data quality, and ensure alignment with the Data Governance Framework.

   c. **TBC:** The Data Management team are currently discussing inclusion in the pilot with three business areas all of which are deemed to hold critical data sets.

6. A review of the Data Governance Framework was conducted. As a result of this review a Version 2 of the Data Governance Maturity Activities (see Annex 3) will be presented to the Data Governance Committee and subsequently the September 2024 RCC. Key changes to include.

   a. Include key Data SME's from across the business to reduce the risk of inconsistencies (see point 8)

   b. remove the activities linked to Records Management which should not be measured by levels of maturity but by compliance with key controls.

   c. Identification and categorisation of Critical Data Sets.

   d. Breaking down the activities into smaller pieces of work to reduce the burden on the businesses.

7. Data Governance was a key component of the recent HIJ remediation project. An assessment of the work undertaken will be conducted to ensure that those requirements have been incorporated and in line with at least IRRELEVANT maturity obligations.

8. Currently across POL there are many initiatives looking at how we manage and use POL data such as the FDP, MDM, NBIT, EAP and Data Management. It is proposed to bring these areas of expertise together to meet on a regular basis to ensure efficient use of resources, sharing of ideas and a consistent approach to all programmes.

9. Obtaining IRRELEVANT maturity is the objective of the Data Management Team. However, we are also looking to the future and how the use of data can give POL a strategic advantage.

10. AI is being adopted by suppliers and there are existing use cases for AI within the POL enterprise estate. There are multiple requests from grass roots within POL on policy and use of AI within the organisation. Therefore, we need to put controls and management around our use of AI within the business. Chris Darriet-Jones will be presenting a paper to SEG and July 2024 RCC to drive AI maturity within POL. It is our belief that AI, effectively managed, can bring significant operational and commercial benefits to POL and support the organisation to meet its strategy objectives.

Financial Impact

11. At this point in time the Data Management Team are asking for no additional funding to support the work needed to reach IRRELEVANT maturity for data governance. However, for maturity to be sustainable then POL will need to consider investment for automated Data Cataloguing and Quality tooling. The ARC will be kept informed on requirements with a business case for any additional funding likely to be included for the financial year 2025-26.

12. The activities of work that need to be undertaken by the business are likely to put a strain on resources as some of the activities are resource intensive. The Data Management Team has a dedicated resource to support the activities and advise on how best to meet the required level of maturity. However, demands for their time are expected to be high, hence why it is proposed to have a staggered roll out of the IRRELEVANT activities.

Risk Assessment, Mitigations & Legal Implications

13. There are two key Intermediate Risks identified and currently worked through SNOW. The Risks are that inadequate Data Governance for Unstructured and Structured Data could lead to legal, regulatory, and statutory infractions. In addition, failure to develop POLs data governance culture could impact on the HIJ remediation work and Phase 7 of the Inquiry.

14. At a local level, these risks should be replicated on business risk registers, and bespoke risks based on criticality of data sets with clear sustainable action plans to reduce risk exposure.

15. There is a risk that all data sets may not be captured as part of the IRRELEVANT activities as Deputy Data Sponsors are reliant on their businesses identifying and recording data sets they own. To help mitigate this Data Management is now part of the formal Gating process with no project, programmes or change initiatives being allowed to progress without completion of at least IRRELEVANT IRRELEVANT maturity and a commitment to reach IRRELEVANT if it involves a critical data set within prescribed timeframes.

16. We believe that current resourcing levels can maintain a controlled roll out of IRRELEVANT activities. However, this is being monitored to ensure that support to businesses is sufficient and not causing delays to their progress.

17. As identified previously the remediation work needed to reach maturity will place a resource challenge on the business. Therefore, work on the IRRELEVANT activities need to be balanced against requirements to operate in a business-as-usual mode. To mitigate this the Data Management Team will support the Deputy Data Sponsors in their creation of a workplan where activities will be broken down into discrete manageable activities.

18. Due to inconsistencies to key terminologies and definitions POL does not currently have a consistent and reliable approach to data management. This leads to uncertainty and impacts the quality of data held by PO. As set out above key data SMEs from across the business will form part of the Data Governance Committee to reduce this risk and in addition will meet monthly to develop a standardisation of key definitions.

Stakeholder Implications

19. The biggest implication for stakeholders on maturity IRRELEVANT is the impact that the required work will have across the business. We will work with the various stakeholders to minimise disruption as much as is possible. As a result of ongoing business obligations, a flexible and fluid approach to delivery will need to be adopted.

20. There is a potential impact for other areas across the IT community as businesses call on areas such as Service Delivery and Cyber Security to provide support and assistance in some of the activities to be undertaken. The Data Management Director is meeting with the Service Director, newly appointed CISO and other key stakeholders to make them aware of the next stages.

Next Steps & Timelines

21. Data Management presented their proposals to the Data Governance Committee and the Risk and Compliance Committee for notification and discussion before being presented to the May ARC.

22. In Q1 24-25 meet with SEG members and Deputy Data Sponsors for those areas involved in the pilot for activities leading to Levels 3 & 4 maturity.

23. In Q2 24-25 work with Key Stakeholders involved with data across POL to create the sub-committee of the Data Governance Committee to ensure that a sustainable, scalable, and consistent approach is adopted to the management of data across all business functions.

24. In back end of Q1 24-25 convene a half day workshop to take those areas involved in the Level 3 & 4 Pilot through the next round of activities. This meeting will include other key stakeholders recognised in the previous point above.

25. In H1 24-25 work with the Inquiry and Remediation Unit to complete Level 2 Maturity to bring them into line with rest of POL.

26. In Q1 24-25 working with the Records Manager develop an Accountability Framework for Records Management for adoption across all POL business areas.

27. As a result of the Assurance of the HIJ programme being conducted by the Group Assurance Team there may need to be additional changes made to the Data Governance Framework. If any gaps are identified, then these will be added to the Data Governance Maturity Dashboard.

Appendix 1

Data Governance Maturity Dashboard – Level 2

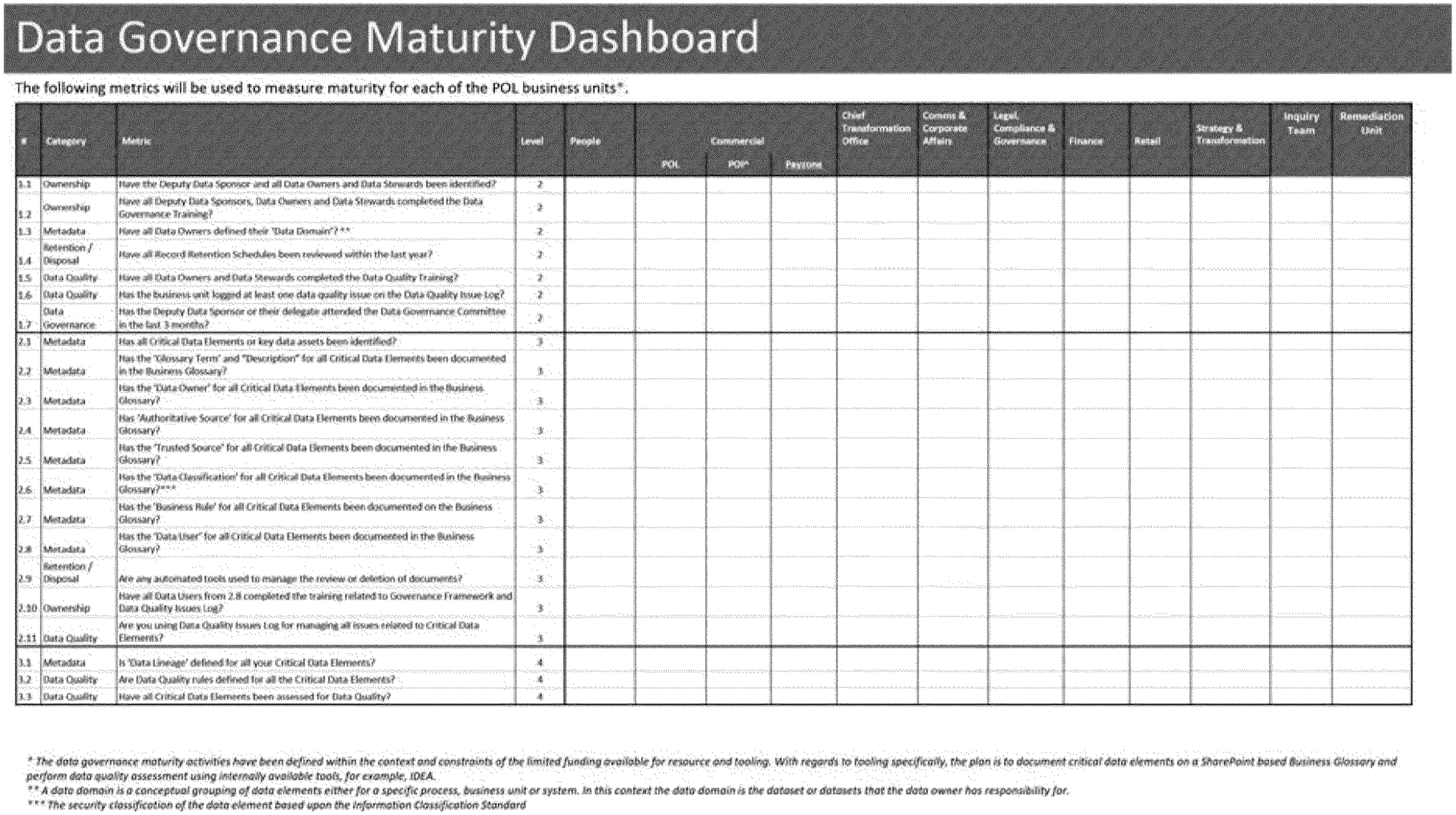
Status as at COB 10-05-2024

#	Category	Metric	People	Commercial***			Chief Transformation Office	Comms & Corp Affairs	Legal, Compliance & Governance	Finance	Retail	Strategy & Transformation	Inquiry Team	Remediation Unit
				POL	POI^	Payzone								
1.1	Ownership	Have the Deputy Data Sponsor and all Data Owners and Data Stewards been identified? ^^												
1.2	Ownership	Have all Deputy Data Sponsors, Data Owners and Data Stewards completed the Data Governance Training?												
1.3	Metadata	Have all Data Owners defined their 'Data Domain'? **	▨		▨	▨		▨					■	■
1.4	Retention / Disposal	Have all Record Retention Schedules been reviewed within the last year?			▨	▨	■	■					■	■
1.5	Data Quality	Have all Data Owners and Data Stewards completed the Data Quality Training?											■	■
1.6	Data Quality	Has the business unit logged at least one data quality issue on the Data Quality Issue Log?			▥	▥		▥					■	■
1.7	Data Governance	Has the Deputy Data Sponsor or their delegate attended the Data Governance Committee in the last 3 months?												■

** The data governance maturity activities have been defined within the context and constraints of the limited funding available for resource and tooling. With regards to tooling specifically, the plan is to document critical data elements on a SharePoint based Business Glossary and perform data quality assessment using internally available tools, for example, IDEA.*
*** A data domain is a conceptual grouping of data elements either for a specific process, business unit or system. In this context the data domain is the structured dataset(s) that the data owner has responsibility for.*
**** Commercial as a business unit has been split into three to consider Post Office Limited, Post Office Insurance (POI) and Payzone as different entities.*
^ Data Governance Framework planned to be presented to Post Office Insurance ARC in January 2024 for approval (Agenda slot TBC). Engagement in progress with Ian Holloway to progress rollout ahead of this.
^^ It is currently not possible to provide assurance that data owners for all datasets within the business have been identified; this is because there is not a complete list of all datasets that exist within the organisation. Business Units should identify Data Owners on a reasonable endeavours basis.
~ Percentage denotes the number of Data Owners that have completed their submissions on the Dataset Inventory and have been reviewed by the Data Management Team.
~~ Percentage denotes the number of Data Owners that have completed their submissions on the Record Retention Schedule and have been reviewed by the Data Management Team. Red RAG status denotes business units which have not started to provide any updates for the Record Retention Schedule.

Key:	
■	Not Started
	In Progress
▨	Data Owners completed, to be signed off
	Complete
▥	Not Applicable

Appendix 2



Data Governance Maturity Dashboard

The following metrics will be used to measure maturity for each of the POL business units*.

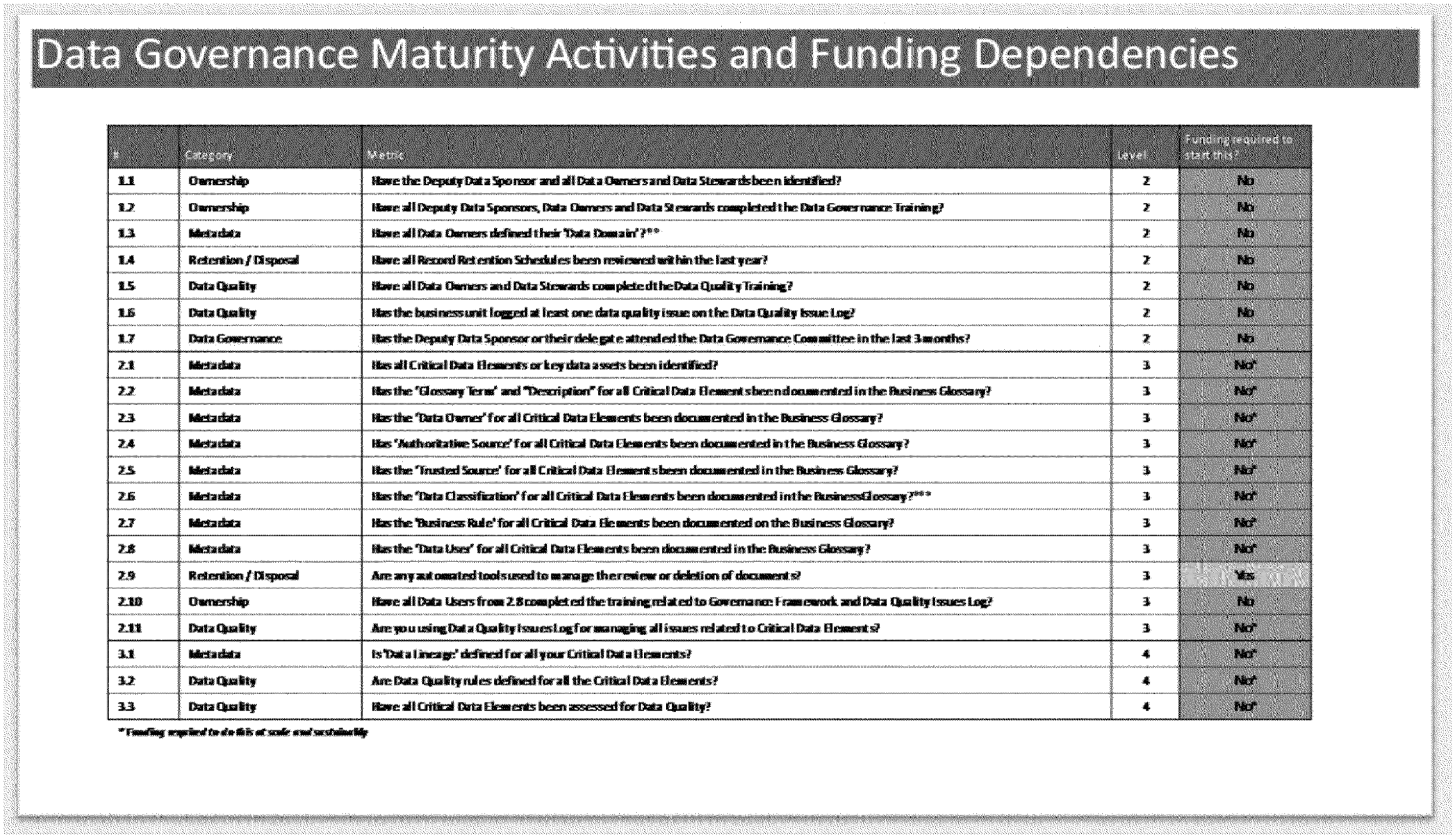
#	Category	Metric	Level	People	Commercial			Chief Transformation Office	Comms & Corporate Affairs	Legal, Compliance & Governance	Finance	Retail	Strategy & Transformation	Inquiry Team	Remediation Unit
					POL	POI^	Payzone								
1.1	Ownership	Have the Deputy Data Sponsor and all Data Owners and Data Stewards been identified?	2												
1.2	Ownership	Have all Deputy Data Sponsors, Data Owners and Data Stewards completed the Data Governance Training?	2												
1.3	Metadata	Have all Data Owners defined their 'Data Domain'? **	2												
1.4	Retention / Disposal	Have all Record Retention Schedules been reviewed within the last year?	2												
1.5	Data Quality	Have all Data Owners and Data Stewards completed the Data Quality Training?	2												
1.6	Data Quality	Has the business unit logged at least one data quality issue on the Data Quality Issue Log?	2												
1.7	Data Governance	Has the Deputy Data Sponsor or their delegate attended the Data Governance Committee in the last 3 months?	2												
2.1	Metadata	Has all Critical Data Elements or key data assets been identified?	3												
2.2	Metadata	Has the 'Glossary Term' and "Description" for all Critical Data Elements been documented in the Business Glossary?	3												
2.3	Metadata	Has the 'Data Owner' for all Critical Data Elements been documented in the Business Glossary?	3												
2.4	Metadata	Has 'Authoritative Source' for all Critical Data Elements been documented in the Business Glossary?	3												
2.5	Metadata	Has the 'Trusted Source' for all Critical Data Elements been documented in the Business Glossary?	3												
2.6	Metadata	Has the 'Data Classification' for all Critical Data Elements been documented in the Business Glossary?***	3												
2.7	Metadata	Has the 'Business Rule' for all Critical Data Elements been documented on the Business Glossary?	3												
2.8	Metadata	Has the 'Data User' for all Critical Data Elements been documented in the Business Glossary?	3												
2.9	Retention / Disposal	Are any automated tools used to manage the review or deletion of documents?	3												
2.10	Ownership	Have all Data Users from 2.8 completed the training related to Governance Framework and Data Quality Issues Log?	3												
2.11	Data Quality	Are you using Data Quality Issues Log for managing all issues related to Critical Data Elements?	3												
3.1	Metadata	Is 'Data Lineage' defined for all your Critical Data Elements?	4												
3.2	Data Quality	Are Data Quality rules defined for all the Critical Data Elements?	4												
3.3	Data Quality	Have all Critical Data Elements been assessed for Data Quality?	4												

** The data governance maturity activities have been defined within the context and constraints of the limited funding available for resource and tooling. With regards to tooling specifically, the plan is to document critical data elements on a SharePoint based Business Glossary and perform data quality assessment using internally available tools, for example, IDEA.*

*** A data domain is a conceptual grouping of data elements either for a specific process, business unit or system. In this context the data domain is the dataset or datasets that the data owner has responsibility for.*

**** The security classification of the data element based upon the Information Classification Standard*

Appendix 3



Data Governance Maturity Activities and Funding Dependencies

#	Category	Metric	Level	Funding required to start this?
1.1	Ownership	Have the Deputy Data Sponsor and all Data Owners and Data Stewards been identified?	2	No
1.2	Ownership	Have all Deputy Data Sponsors, Data Owners and Data Stewards completed the Data Governance Training?	2	No
1.3	Metadata	Have all Data Owners defined their 'Data Domain'?**	2	No
1.4	Retention / Disposal	Have all Record Retention Schedules been reviewed within the last year?	2	No
1.5	Data Quality	Have all Data Owners and Data Stewards completedthe Data Quality Training?	2	No
1.6	Data Quality	Has the businessunit logged at least one data quality issue on the Data Quality Issue Log?	2	No
1.7	Data Governance	Has the Deputy Data Sponsor or their delegate attended the Data Governance Committee in the last 3 months?	2	No
2.1	Metadata	Has all Critical Data Elements or key data assets been identified?	3	No*
2.2	Metadata	Has the 'Glossary Term' and "Description" for all Critical Data Elements been documented in the Business Glossary?	3	No*
2.3	Metadata	Has the 'Data Owner' for all Critical Data Elements been documented in the Business Glossary?	3	No*
2.4	Metadata	Has 'Authoritative Source' for all Critical Data Elements been documented in the Business Glossary?	3	No*
2.5	Metadata	Has the 'Trusted Source' for all Critical Data Elements been documented in the Business Glossary?	3	No*
2.6	Metadata	Has the 'Data Classification' for all Critical Data Elements been documented in the BusinessGlossary?***	3	No*
2.7	Metadata	Has the 'Business Rule' for all Critical Data Elements been documented on the Business Glossary?	3	No*
2.8	Metadata	Has the 'Data User' for all Critical Data Elements been documented in the Business Glossary?	3	No*
2.9	Retention / Disposal	Are any automated tools used to manage the review or deletion of documents?	3	Yes
2.10	Ownership	Have all Data Users from 2.8 completed the training related to Governance Framework and Data Quality Issues Log?	3	No
2.11	Data Quality	Are you using Data Quality Issues Log for managing all issues related to Critical Data Elements?	3	No*
3.1	Metadata	Is 'Data Lineage' defined for all your Critical Data Elements?	4	No*
3.2	Data Quality	Are Data Quality rules defined for all the Critical Data Elements?	4	No*
3.3	Data Quality	Have all Critical Data Elements been assessed for Data Quality?	4	No*

* Funding required to do this at scale and sustainably

[redacted]

POST OFFICE

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Management of Physical Branch Data	**Meeting Date:**	Tuesday 21st May 2024
Author:	Kayleigh Dodd – Digital / Physical Records Manager	**Sponsor:**	Chris Russell – Interim Data Management Director

5

Input Sought: Noting and discussion.

The ARC is asked to note and discuss the approach to the management of physical (i.e., unstructured) data held in Branch.

Executive Summary

The report [3.0_POL_RCC_Unstructured_Data_20230314_FINAL] was submitted to RCC and subsequently ARC in March 2023, drawing attention to some of the risks presented to POL through the poor management of physical data. The ARC requested an update on the plan to address these risks, which is the topic of this paper, with a particular focus on the poor management of physical and digital data in POL's Branches. Management of physical and digital data in back-office areas of POL is not considered in this paper.

Note that this risk is currently summarised under RK0021709 within ServiceNow - *Poor management of unstructured information (hard copy material and unstructured digital information such as documents saved in SharePoint).* The risk is currently outside of appetite and tolerance. The specific risk in relation to the management of Branch data is in the process of being defined and agreed in terms of the risk ownership, with an expectation that an update can be provided at the September ARC.

Report

What risk is presented through the poor management of physical data across the Branch network?

1. POL has more than 11,500 Branches each generating and storing a significant volume of physical data. This data includes but is not limited to:
    - Branch trading reports (retained for 6 years)
    - MoneyGram records – **containing customer data** (retained for 5 years)
    - ATM weekly balancing statements (retained for 2 years)
    - Banking deposits/withdrawal receipts (retained or 2 years)
    - Passport receipts (retained for 2 years)
    - Remittances in/out receipts (retained for 2 years)
2. In some Branches this paperwork is stored in a way that increases the risk that the integrity of the data may be compromised (e.g., documents do not appear to be disposed of in a timely fashion with little ability to identify when a disposal date has been reached, etc.). Postmasters must fund any disposal costs themselves (excl. DMBs) and paperwork is only archived with POL's storage provider Oasis when they close. These factors lead to

minimal disposal taking place and over retention of data on site, and a consequent risk of loss or compromise to this data. No auditing activity takes place on how Branches manage their physical data.

3. When a Branch does close and is required to archive paperwork, there is little control over the process with many not following guidance. This results in boxes of unindexed records and often rubbish arriving at Oasis for storage, creating a further risk that POL does not have knowledge of what data it holds in archive. This also has a cost impact on POL.

4. Where personal data is referenced in Branch records, POL is contractually responsible as a data processor for handling this in accordance with the Data Protection Act, with the Postmaster recorded as a sub-processor.

5. The risks associated with poor management of physical data are referenced in Appendix 1. Whilst the likelihood of one of these risks materialising is considered minimal in relation to Branch data specifically, there remains a material risk of non-compliance to the Data Protection Act for products such as MoneyGram, where over retention or accidental disclosure of personal data could lead to significant fines and reputational damage to POL.

What steps are the Data Management Team taking in relation to this risk?

6. Historically branches have been required to retain extensive physical transactional records on site for a number of years, even though these requirements have not been reviewed or updated in some time. This means it is currently unclear what records must be retained, for how long and for what reason. Until these requirements are updated and documented, Branches will continue to retain physical records in the manner they have historically done so and potentially when POL has no legal, regulatory or business reason to require it.

7. Through the Data Governance Framework, the Data Management Team are formalising the accountability, ownership and responsibility for records retained in Branch. Initial discussions have been held between with Deputy Data Sponsors for Retail, Commercial and Finance which a view to understanding who within these units (or elsewhere across POL) requires physical records to be retained within Branches. It is possible that there is no longer a requirement to retain many of these physical records due to process changes.

8. Once Data Owners have been assigned, this ownership and the retention requirements of any records will be documented in the POL Record Retention Schedules. As with all other business records across POL, the ongoing management of records is the responsibility of the Data Owner, with the accountability assigned to the relevant Data Sponsor. Any risk identified in relation to this must be raised, explored and mitigated by the Data Owner. This includes the way any physical records are managed and disposed of within Branches.

9. The Data Management Team will offer support and guidance with practical ways to manage physical records, especially those that are not under the direct control of the Data Owner. Once the retention requirements have been confirmed, POL will explore the opportunity for NBIT to include the functionality to retain relevant records digitally, rather than in a physical format (i.e., in circumstances where retention continues to be required).

Risk Assessment

The Board agreed risk appetite is AVERSE in relation to risks materialising from unauthorised access to sensitive data, unauthorised changes to data and ineffective processes and procedures for the management of data. As things currently stand POL is outside of risk appetite which potentially has legal, contractual and reputational consequences. The risk is not considered significantly out of appetite through the management of Branch data alone, but in conjunction with the management of data across the organisation as a whole.

Legal Implications

[redacted]

The Data Management Team are seeking to address the accountabilities point through the Data Governance Framework and clear definition of data roles and responsibilities. Appendix 1 sets out more detailed information on the risks and their potential impact, although as previously stated these risks are considered more likely to crystallise from the poor management of physical and digital data in back-office areas of POL rather than from Branch data.

Stakeholder Implications

Any changes proposed to the way in which Postmasters manage paperwork within branch through to disposal must be led by the Data Owner and fully scoped with the Retail Team with Postmaster engagement. Reduced retention requirements would be expected to be welcomed by Postmasters due to the time saved and efficiencies from freeing up space otherwise used for records' storage.

Next Steps & Timelines

A workshop will be arranged with colleagues from the Commercial, Retail and any other relevant teams identified to:

- Agree on the ownership of any physical records stored in Branch.
- Review the legal, regulatory or business reason to retain these and update the relevant Record Retention Schedules with these requirements.
- Refresh Postmaster guidance in this area.
- Assign ownership of any risk in relation to the management of physical Branch records and collaboratively explore mitigation options.

It is recommended that this action be kept open to maintain the focus of the ARC that this issue needs to be addressed, with a recommendation that the Data Management Team provide an update at the September ARC.

5

Appendix 1 – Risks associated with poor management of physical data.

Potential risks	Potential Impact
Breach of legal obligations of disclosure associated with the Inquiry. For example, inability to identify and locate relevant documents to respond to the Inquiry's requests.	• Criminal offence for any person who fails to produce any documents in his custody or under his control that relate to a matter in question at the Inquiry. • Criminal offence for any person who intentionally suppresses or conceals a document that is relevant or intentionally alters or destroys any such document. • Risk of Inquiry reaching adverse inferences from inability to identify and locate documents. • Negative press coverage and/or reputational damage.
Non-conformance with or a material breach of UK GDPR, as well as the Data Protection Act 2018 legislation For example, unauthorised access to and use of sensitive personal data held securely in the Network, resulting in customer detriment.	• Maximum fine of £17.5m or 4% of annual turnover, depending on which is the greater amount, and significant reputational impact.
Breach of criminal disclosure requirements in the CCRC, CACD and triage processes	• Could result in the CCRC or CACD finding against POL, which could result in it having to pay damages. • Adverse costs orders against POL.
Breach of POL's disclosure obligations in civil litigation For example, being unable to locate or identify documentary evidence to support POL's legal position in civil proceedings.	• Could result in POL losing a civil claim, which could result in it having to pay damages, as well as its own legal costs and the other party's legal costs. • Inability to comply with court disclosure orders. • Adverse costs orders against POL regardless of the outcome of a judgment.
Breach of regulatory obligations For example, unable to comply with Regulator's order to deliver up certain categories of documents.	• Risk of Regulator drawing adverse inferences from POL failure to identify, locate and provide documents ordered, which could result in negative findings in a Regulator's investigation. • Data Protection Officer may not be able to give annual regulatory confirmations to ICO.

Potential risks	Potential Impact
	• Negative statements from the Regulator (ICO) as a result of failure. • Negative press coverage and/or reputational damage.
Breach of contractual obligations For example, POL being unable to comply with audit rights in a contract, or to provide required regular reporting to evidence meeting its contractual obligations.	• Potential contractual damages payable by POL. Value will depend on each contract's limitation caps.
Non-conformance with or a material breach of Freedom of Information Act 2000 For example, inability to identify and locate relevant documents to respond to FOIA requests.	• Negative statements from the Regulator (ICO) as a result of failure. • Negative press coverage and/or reputational damage.

Post Office Limited - Document Classification: INTERNAL

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Transformation Office Update May 2024	**Meeting Date:**	21 May 2024
Author:	Jo Welch, Head of Change and Risk Assurance	**Sponsor:**	Tim McInnes, Strategy and Transformation Director

Input Sought:

1. For **noting**, a Strategy and Transformation Update.

Executive Summary

6

Since our last update in September 2023 the S&T Change and Risk Assurance function has focussed its efforts on *inter alia*: (i) delivery against our Integrated Assurance Schedule; (ii) working with Central Risk to update our risk profile and intermediate level risks and (iii) reviewed and refreshed our control framework.

Over the same period it is worth RCC noting that Data Governance and Management has now moved its reporting line under S&T, and that S&T is now part of POL's CFO Function reporting to SEG through the Interim CFO. These structural changes are not considered in this note but can be covered in a verbal update if required by the Committee.

S&T Update

Assurance Undertaken Against the Change Assurance Framework

1. Since the last update Project Health-checks by Portfolios have been introduced, and four of these have now been completed (i.e. Data Enablement Programme, Project Darwin, Auto-stock REM and Future DMBs). This has resulted in a marked improvement in project control data and the quality of project status reporting for the reviewed activities, with less rework required during the monthly performance reporting cycle (e.g. reports for IADG, UKGI and Investment Committee). There is a desire to continue this cadence of reviews into FY24/25 however tightened resourcing arrangements and associated pressures might make this challenging. Current planned assurance activities are detailed in Annex 1.

2. Independent assurance reviews that have been completed by the Change Risk Assurance team include four assurance project reviews (i.e. Copper Stop Sell, Payment Electronic Devices (PEDs, Project Columbus, and Belfast Exit, two Thematic Reviews Project Closure Process and Project Lessons Learnt) and one facilitated risk workshop (i.e. Fit & Proper). A summary of these activities is listed in Annex 2. Common themes identified in these reviews / workshops relate to effectiveness of sponsorship arrangements, membership of steering committee to include suppliers for increased oversight, the lack of a consistent business change management framework to improve outcome success and the need to drive improved co-ordination across projects / programmes to minimise impact on Branches and organisational capabilities to implement. Business risks identified during change assurance reviews outside of S&T influence & control and transferred to business teams has been provided in the reading room.

3. In addition, following the recent POHIT Inquiry workshop, it is clear that work is needed to ensure alignment of SPMP to the Change Excellence Framework and POL's Business Change Policy (following recent re-planning). In particular improved visibility of reporting

will enable robust challenge to provide S&T confidence in SPMP, and help support a wider integrated picture of cross-POL change.

Risk Workshop

4. Central Risk facilitated a risk workshop using industry benchmarks and standard risk management practices to challenge existing risks and to identify potential gaps. Several duplicate risks were retired, while others were moved from intermediate to local oversight, with ownership transferred to drive accountability at a portfolio level for both unexpected costs & data quality. As a result of the review the total number of intermediate risks has decreased from five to two; three of the prior five have been retired as their scope duplicated other local risk, two have been realigned so that they will now be managed at local level, and two risks that were previously managed at a local level have now been elevated to intermediate level (i.e. a net reduction of three intermediate risks).

5. Updates against the two new intermediate risks are set out below. See Annex 3 for further details of these new intermediate risks.

6. ARC are reminded Change risks are reported monthly to IADG and UKGI, and these are also submitted to the Investment Committee for visibility. For completeness these have been provided in the reading room.

Controls Refresh

7. To ensure our controls are aligned to the correct risk we have remapped our controls to our risks. These controls have also been reviewed in full control Owners resulting in an overall reduction in the number of controls from 36 to 22. A number were retired as deemed process activities and not controls (not directive, detective, preventive, or corrective). See Annex 4. The next annual review of controls is September 2024.

RK0021313 - Incorrect Stakeholder Engagement (TBA)

8. This risk has now been elevated to intermediate level (it was previously a local risk) in recognition that the sponsorship role on some projects has on occasion been incorrectly assigned (e.g. Copper Stop Sell, PED Replacement), which has impacted successful delivery as well as the successful transition of these activities into BAU operation. This risk is undergoing assessment, so its impact / likelihood scores are still to be determined.

9. The recent assurance reviews of Copper Stop Sell and PED Replacement identified that sponsorship does not always meet assurance standards and sponsorship expectations under the Change Excellence Framework, as sponsorship in these areas in particular had been assigned to CIO rather than Retail (i.e. sponsorship was separated from end outcomes). These contrast to successful sponsorship arrangements, such as in Lottery Transition (PIR due to be shortly published), where sponsorship focused on the end outcome has helped to support successful delivery. Sponsorship for these projects has now been changed.

10. Furthermore in response to a recent Internal Audit (Copper Stop Sell) which identified that business readiness assessment needed strengthening with addition clarity being required to Stakeholder Gating the Terms of Reference on members' responsibilities, to ensure the areas they represent are ready to accept change, where relevant. Although this has always been in scope of the Stakeholder Gating process these changes make the responsibility explicit. Once complete all members will be retrained accordingly.

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

RK0022259 - Dependencies Between Programmes / Projects Not Understood (TBA)

11. This risk has been previously been recognised in S&T as a Change Risk (i.e. managed within the project management module of ServiceNow, not the GRC module which captures Business Risk) and it was reported as such, however following the Risk and Controls Refresh this has now been raised as an intermediate risk due to the number of significant, complex and interdependent programmes currently in-flight across POL (e.g. SPMP (and other Horizon Replacement workstreams), Copper Stop Sell, Auto-Stock REM, MDM Credence, etc.). If interdependencies across these activities are not fully understood and managed this could have a material negative impact on change delivery schedules, including benefits and timelines, while also having a negative operational impact on internal teams and Postmasters. This risk is undergoing assessment, so its impact and likelihood score is still to be determined.

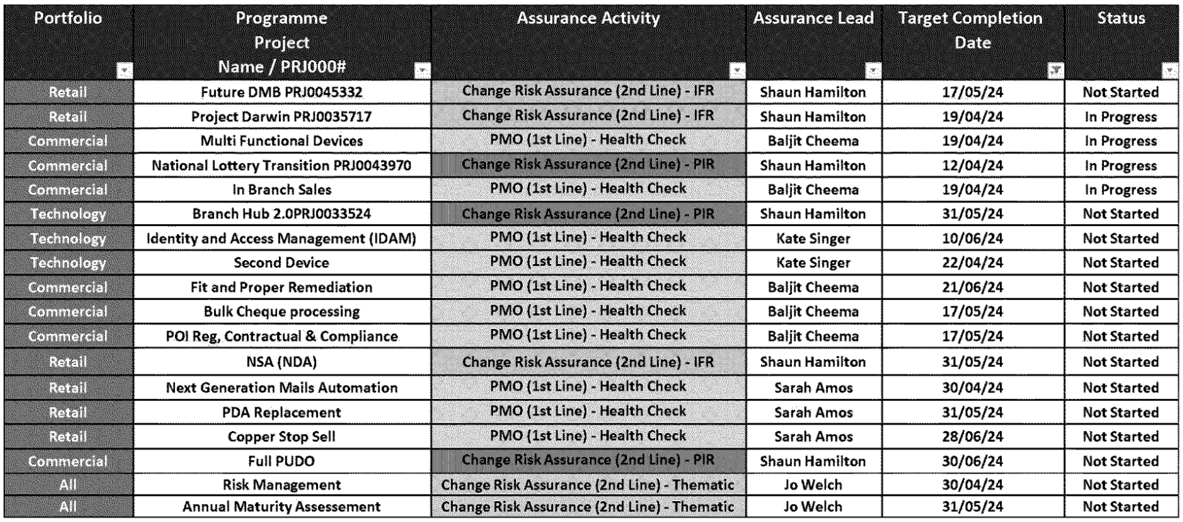
6

12. To help provide better oversight of interdependencies the Strategic Alignment Module has now been implemented in ServiceNow, which enables project-to-project dependencies to be captured on delivery roadmaps and aligns change projects to strategic priorities, business goals and targets. This has also increased transparency which is helping identify data quality issues which are now being remediated.

13. In addition the ServiceNow Project Planning Workspace has been upgraded to a more user-friendly interface, which enables task level project-to-project dependencies to be linked, automatically informing projects if predecessor tasks slip. Compliance against these and other planning standards remains a focus of all portfolios in S&T with some areas more advanced than others; SPMP in particular is considered a high risk as this is managed outside POL's chosen strategic PPM tooling, constraining POL's ability to have a single integrated view of all change activity (including but not limited to dependencies) taking place across the business.

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

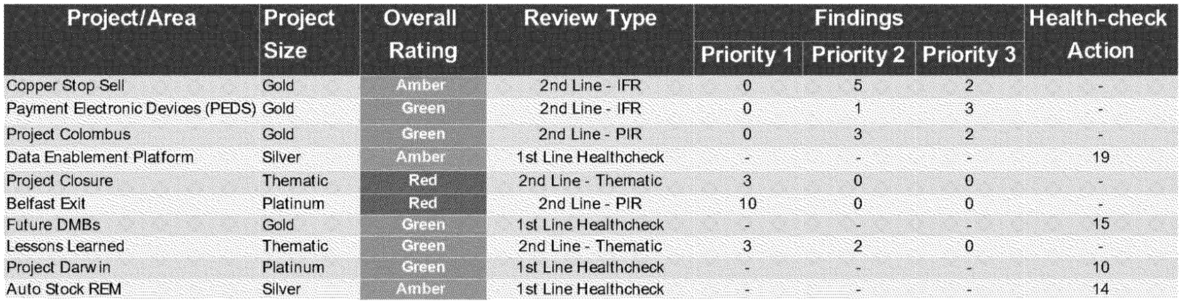
Annex 1: Change Assurance Reviews Planned in Next Quarter*



Portfolio	Programme Project Name / PRJ000#	Assurance Activity	Assurance Lead	Target Completion Date	Status
Retail	Future DMB PRJ0045332	Change Risk Assurance (2nd Line) - IFR	Shaun Hamilton	17/05/24	Not Started
Retail	Project Darwin PRJ0035717	Change Risk Assurance (2nd Line) - IFR	Shaun Hamilton	19/04/24	In Progress
Commercial	Multi Functional Devices	PMO (1st Line) - Health Check	Baljit Cheema	19/04/24	In Progress
Commercial	National Lottery Transition PRJ0043970	Change Risk Assurance (2nd Line) - PIR	Shaun Hamilton	12/04/24	In Progress
Commercial	In Branch Sales	PMO (1st Line) - Health Check	Baljit Cheema	19/04/24	In Progress
Technology	Branch Hub 2.0PRJ0033524	Change Risk Assurance (2nd Line) - PIR	Shaun Hamilton	31/05/24	Not Started
Technology	Identity and Access Management (IDAM)	PMO (1st Line) - Health Check	Kate Singer	10/06/24	Not Started
Technology	Second Device	PMO (1st Line) - Health Check	Kate Singer	22/04/24	Not Started
Commercial	Fit and Proper Remediation	PMO (1st Line) - Health Check	Baljit Cheema	21/06/24	Not Started
Commercial	Bulk Cheque processing	PMO (1st Line) - Health Check	Baljit Cheema	17/05/24	Not Started
Commercial	POI Reg, Contractual & Compliance	PMO (1st Line) - Health Check	Baljit Cheema	17/05/24	Not Started
Retail	NSA (NDA)	Change Risk Assurance (2nd Line) - IFR	Shaun Hamilton	31/05/24	Not Started
Retail	Next Generation Mails Automation	PMO (1st Line) - Health Check	Sarah Amos	30/04/24	Not Started
Retail	PDA Replacement	PMO (1st Line) - Health Check	Sarah Amos	31/05/24	Not Started
Retail	Copper Stop Sell	PMO (1st Line) - Health Check	Sarah Amos	28/06/24	Not Started
Commercial	Full PUDO	Change Risk Assurance (2nd Line) - PIR	Shaun Hamilton	30/06/24	Not Started
All	Risk Management	Change Risk Assurance (2nd Line) - Thematic	Jo Welch	30/04/24	Not Started
All	Annual Maturity Assesement	Change Risk Assurance (2nd Line) - Thematic	Jo Welch	31/05/24	Not Started

*This does not include assurance reviews commissioned through IADG or Gating

Annex 2: Change Assurance Reviews Undertaken Since Last Update



Project/Area	Project Size	Overall Rating	Review Type	Findings			Health-check Action
				Priority 1	Priority 2	Priority 3	
Copper Stop Sell	Gold	Amber	2nd Line - IFR	0	5	2	-
Payment Electronic Devices (PEDS)	Gold	Green	2nd Line - IFR	0	1	3	-
Project Colombus	Gold	Green	2nd Line - PIR	0	3	2	-
Data Enablement Platform	Silver	Amber	1st Line Healthcheck	-	-	-	19
Project Closure	Thematic	Red	2nd Line - Thematic	3	0	0	-
Belfast Exit	Platinum	Red	2nd Line - PIR	10	0	0	-
Future DMBs	Gold	Green	1st Line Healthcheck	-	-	-	15
Lessons Learned	Thematic	Green	2nd Line - Thematic	3	2	0	-
Project Darwin	Platinum	Green	1st Line Healthcheck	-	-	-	10
Auto Stock REM	Silver	Amber	1st Line Healthcheck	-	-	-	14

*Health-checks do not prioritise their actions so reported in a separate column.

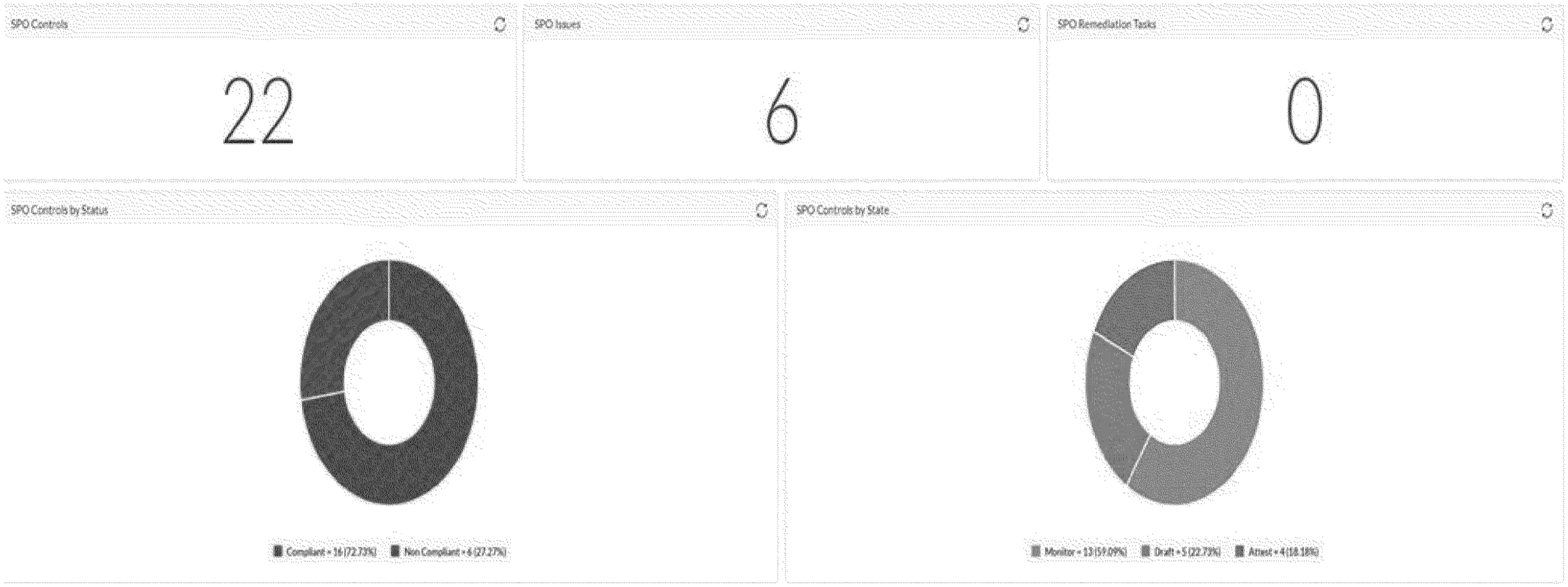
POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Annex 3: Intermediate Risks Position April 2024

Risk ID	Title	Description	Previous Risk Score	Owner
RK0021313	Ineffective stakeholder engagement.	**CAUSE:** Due to the lack of willingness, education, defined criteria, inconsistent project/sponsor ownership and processes being not robust enough **EVENT:** There is a risk of incorrect stakeholders (e.g. sponsors, Postmasters) engagement, **IMPACT:** which may result in inadequate communication with key stakeholders, partial delivery of projects/programmes outcomes, incorrect constitution of SteerCo, projects missed, negative impact on business continuity, reduction of business benefits, misaligned objectives or expectations between interested parties.	New	George Cross
RK0022259	Dependencies between programmes/ projects not understood.	**CAUSE:** Due to lack of transparent and accurate plans with programmes not following the Change Excellence Framework, detailed plans not available, and programmes being allowed to operate outside of standard process, **EVENT**: There is a risk that dependencies between programmes/projects and therefore potential conflicting objects and decisions effects on other projects/programmes are not understood, **IMPACT**: which may result in significant delivery delays, additional costs and delayed benefits realisation.	New	Tim McInnes
RK0022302	Inability to deliver complex programmes	**Cause: :** As business needs evolve, including the requirements of increasingly complex and interdependent transformation initiatives (SPMP, Copper Stop Sell, PEDs etc) POL's change governance framework will need to mature to accommodate (e.g. business change management, business capacity to accept change, better co-ordination of branch impacting activities, visibility of dependencies and key decisions, etc.). **Event:** There is the risk that complex programmes may fail to deliver their expected outcome, to cost, quality or schedule **Impact:** which may impact POL ability to deliver its strategic priorities or remediate significant enterprise risks.	New	Tim McInnes

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Annex 4: SPO Controls Assessment (April 2024)



SPO Controls: 22

SPO Issues: 6

SPO Remediation Tasks: 0

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Post Office Limited (POL) and Post Office Insurance (POMS) relationship and obligations	**Meeting Date:**	21 May 2024
Author:	Ed Dutton Product Portfolio Director	**Sponsor:**	Owen Woodley, Deputy Chief Executive

Input Sought: Decision

The Committee is asked to **note** the attached paper regarding the relationships between Post Office Limited (POL) and its regulated subsidiary entity, Post Office Insurance (Post Office Management Services Limited - POMS)

Executive Summary

This paper aims to remind POL ARC members of the relationship(s) between POL and POMS, the complexities, and potential conflicts it brings, and the obligations on parties as a result. It also reflects on recent changes in regulatory scrutiny of such relationships, some of the recent events and challenges associated with it, the progress made in improving aspects of it and further plans to continue doing so.

7

Report

The relationship

1. The relationship between POL and POMS is multifaceted, and each element of the relationship brings with it rights and obligations which need appropriate navigation and respect. In other words, individuals in either party will sometimes benefit from consideration or indeed precise thinking as to which role an individual or firm is operating in when managing business matters.
2. There are four main aspects to the relationship:
    a. **Post Office Insurance (Post Office Management Services Ltd) (POMS) is a subsidiary of Post Office Limited (POL).** In this respect, POL may act as the group owner of POMS, delivering the Groups strategy and ensuring the subsidiary is performing to group standards, etc. There are also some reserved matters/control rights retained by group, with the need for POL Remco approval of appointments to subsidiary Boards being a good example.
    b. **POMS is an Insurance Intermediary statutory entity, authorised and regulated by the FCA**, which it must be to co-manufacture and distribute Insurance products. This means that POMS must be able to demonstrate independent governance and an ability to operate on its own. POMS has its own Board with Chair, NEDs and an Audit, Risk and Compliance committee.
    c. **POL is an Appointed Representative (AR) to three principal firms, one of which is POMS** (the others being Bank of Ireland and Capital One). Certain regulated activities (mainly branch sales and financial promotions which includes website distribution) are performed by POL on behalf of POMS (and the other principals). It does this as an AR, which allows POL to not be regulated in its own right, but meaning the principal firms take regulatory responsibility for POL activity.

POST OFFICE

That brings with it the need for POMS to effectively oversee POL and the activity it performs. It also hands POMS other obligations – for instance ensuring the management and governance of their AR is performed by fit and proper people.

Note: Regulations regarding the Appointed Representative regime have recently been strengthened and continue to be a focus for the FCA. These changes are outlined further below.

d. **POL provides other services to POMS for it to function**, utilising group departments such as IT (for desktops), legal, company secretarial, HR, digital and so on. These are set out in a multi-services agreement (MSA), with specific services, roles who provide the interface between entities and the service standards expected. This too means POMS must be able to oversee delivery of these services and intervene and escalate if required, to ensure it, as an independent regulated entity is delivering for its customers as it (and regulations) requires.

<u>Potential for conflicts</u>

3. The rights and obligations that each of these aspects of the relationship brings have the potential to create conflicts
4. The obvious generic challenge is POL operates at two different levels in POMS eyes - crudely a 'superior' sense as Group and owner, but in an 'inferior' sense as Appointed Representative and service provider.
5. This means that potentially straightforward conflicts between owner and regulated independent subsidiary have further nuance because the owner is also the appointed representative and/or service provider for which POMS is responsible.
6. Whilst POL is the owner, POMS must be able to demand and oversee that POL performs to the standards and deliver on the obligations required in its other roles. Furthermore, whilst POL as parent sets group strategy and retains some reserved matters, POMS must be able to evidence that POL as unregulated owner does not have undue influence over regulated activity.
7. Conflicts may occur in the normal course of business - such as the priorities and challenges facing POL may lead to group decisions that have a consequential impact on POMS without POMS being considered or informed. In more dramatic terms, such a decision might (or might be perceived to) interfere with POMS independence.
8. Other examples might include that POMS may identify risks that are a priority to mitigate that do not align with POLs risk profile: i.e. what's important to one entity might not be similarly important to another. Or POL becomes aware of something that might impact its fitness and propriety as an AR but does not consider that aspect and does not inform its principals. The current inquiry has amplified this risk recently.
9. Another subtler addition to the challenge is that we have increasingly integrated personnel over the last few years, such that some POL staff are performing roles for POMS alongside other POL roles, where previously POMS consisted of predominantly dedicated staff, employed by POMS.

<u>Increased Regulatory focus on Appointed Representatives</u>

10. Changes to the AR regime were launched in December 2022, hand-in-hand with the new Consumer Duty regulations, which came into force on 31 July 2023. The rules supporting the AR regime and Consumer Duty are designed to reinforce each other in increasing protection for consumers dealing with ARs.

11. The FCA summarise the new obligations on POMS as:
    - ***Enhanced oversight requirements:*** *Apply enhanced oversight of ARs, including ensuring having adequate systems, controls, and resources.*
    - ***Annual self-assessment:*** *Prepare a single document demonstrating compliance with obligations as a principal, identifying any risks and gaps. The firm's governing body should review and sign off this document at least annually.*
    - ***Annual review of AR's activities and business:*** *Annually review information on the ARs' activities and business, including the fitness and propriety of senior management, the ARs' financial position and the adequacy of the principal's controls and resources to effectively oversee the AR.*
    - ***Review oversight approach:*** *Principals should review whether their oversight remains appropriate in certain situations, for example, the size or volume of the AR business involving regulated activity increases significantly in a short period of time.*
    - ***Notification of planned AR appointments:*** *Notify us of an intended AR appointment 30 calendar days before it takes effect. New FCA forms gather more detailed information.*
    - ***Annual reporting:*** *Provide complaints and revenue information for each AR to the FCA on an annual basis and confirm AR details are correct as part of annual attestation.*
12. The FCA have also performed various data gathering exercises and held meetings with some firms (including POMS).
13. There are some specific aspects of the new rules which might apply to POI's relationship with POL, which they describe clearly in their own publication.
14. The first relates to the relative size and scale of principal firm to AR.

".......where an AR or the group in which they operate is disproportionately large relative to the principal, we are concerned this could lead to harm. For example, where a principal becomes overly reliant on an AR to sustain its business, this might undermine the independence and effectiveness of its oversight. The relative size and complexity of larger ARs can also mean a principal does not have sufficient skills and resource to effectively oversee them...."

15. The other is a clear need for POI to have adequate controls over POL's AR activities and means of enforcing compliant delivery by POL.

> *".......To be able to oversee ARs effectively, principals need to consider their oversight arrangements carefully. Principals are required to have 'adequate' controls over the AR's activities, and resources to monitor and enforce an AR's compliance with the relevant requirements that apply to its regulated activities. That assessment must be reviewed at least every 12 months."*

16. Since late 2022, these new rules, and some of the more specific focus areas of the FCA, correctly heightened POMS interest in the effectiveness of their oversight of POL, and POL's delivery as AR (and other service provision).

7

Examples of recent issues

17. Over those last 18 months or so, several challenges have combined with that heightened awareness to create good examples of the need for both parties to understand their respective roles and responsibilities. These issues have generally been resolved successfully, but in many cases, the escalations and time required to do so did not give confidence that POMS was as effectively overseeing its AR or service provider as it would wish.

18. These include:

    a. The first enhanced Fit and Proper checks took too long: The enhanced FCA regulations regarding management and oversight of ARs were implemented by POMS last year as part of a regulatory change programme that included new Consumer Duty rules. The first attempt at the enhanced Fit and Proper checks of POL Executives and Board members was frustratingly slow and took too long to complete. It was not helped by significant changes to personnel, but this gave an impression of an apparent lack of urgency or awareness of importance.

    b. Clarity of POL view on Cyber Risk: POMS is predominantly a digital business and treats Cyber-attack as one if its top risks. It is regularly attacked, and as it has its own IT environments has significantly strengthened its own firewalls, preventative and detective software and its escalation and resolution processes. Last year, on further review of potential vulnerabilities, POMS discovered some acknowledged weaknesses within the POL estate, notably regarding Horizon and Belfast that had not been shared with POMS, meaning POMS were operating outside its risk appetite. It took too long to establish whether POLS view of cyber risk was consistent, was in tolerance with its own appetite and whether POLs plan to mitigate certain vulnerabilities offered sufficient comfort.

    c. Understanding of importance of services provided: within service provision, POMS contracts with POL to receive certain amounts of dedicated resources in various functions, and over an extended period an unfortunate sequence of changes of personnel in different departments combined with a sequence of minor events or poor service provision led to a period of dissatisfaction with POLS service provision and how effective POMS were at overseeing their delivery.

    d. IT controls and procedures: the more recent data access control incident in the NBIT programme, and the speed of its escalation and notification, added a further layer of discomfort that POL inherently has the controls in place to perform its duties to POMS in a satisfactory manner.

    e. There is currently a recruitment process underway to identify a new chairman for POMS. This has clear relevance to potential conflicts. On the one hand, the appointment is a matter reserved to the owner POL and must be approved at POL NomCo, but care must be taken that the AR of POMS is not having undue influence on deciding the members of the principal's board. As POL Nomco retains appointments as a reserved matter, POL may have its own group reasons to advise on candidates it will not approve, but the identification of suitable candidates and the selection process leading to a recommendation for approval must be (and seen to be) performed by the regulated entity independently from its AR, before recommendation to NomCo. Notably, any appointments to FCA regulated subsidiary boards do NOT required DBT/ultimate shareholder approval, unlike many other group director appointments. I will provide a verbal update on the latest progress.

7

19. This combination of several incidents and frustrations did create questions regarding the level of understanding of the nuanced nature of the intercompany relationships and the impact of wider decisions made by the group on the regulated business. Ultimately this has led to this paper being presented at ARC.

20. A range of improvements have been made to improve the interfaces between POL and POMS which means governance and oversight is now generally working well.

Oversight in practice and recent improvements

21. The Owner and AR interface is predominantly managed via governance arrangements: each entity has its own independent board and audit committees and POMS has clear Terms of References reflecting its own responsibilities and reserved matters. POMS has a suite of policies and procedures – not withstanding it formally adopts POL ones whenever it can.

22. There are contractual agreements in place between POL and POMS regarding the AR arrangement and service provisions. These have been recently reviewed and updated.

23. Whilst POL is not regulated, the CEO of POL is recorded as acting in a 'controlled function' by the FCA and carries the responsibility for POL as an AR. POMS has met with Nick to update him on the AR and MSA obligations and the actions taken to oversee them.

24. One (Non-Independent) NED on POMS board (currently me) acts as a shareholder representative. Notwithstanding the need to navigate my own potential conflicts as an employee of the group and AR, portfolio director of all the financial services businesses (including POMS and the other Principals) and director of POMS, this role should act as a conduit between Group/subsidiary and principal/AR. I have recently agreed that I will meet regularly with the senior NED outside formal meetings to ensure the board are aware of any relevant POL activity, where appropriate and necessary.

25. The Senior NED of POMS (who is chair of POMS ARC) already meets regularly with the POL ARC chair to enable sharing of risk, audit and compliance activities in the two entities and POMS updates POL ARC via regular reporting.

26. Beyond these communication channels, we have a documented POMS policy regarding management of conflicts between the entities. This includes recourse to legal advice for POMS board members, and formal escalation routes via POMS shareholder director, or from POMS chair to POL MD, etc)

27. The most recent round of fit and proper checks of POL directors and executives is progressing significantly smoother than the first. All documentation has been received and checks are underway. This is a material and welcome improvement.

28. Specifically, regarding execution of services provided within the MSA, we have identified a role within POL (Finance Director for Commercial) to be a single point of contact for monitoring and escalation, and this has already made a material difference to the ability for POMS to effectively oversee POLS service performance.

29. There are changes to HR personnel underway, including the designated HR support to the POMS board, but it has been pleasing with the early engagement of the need for that focus and the identification of a suitably senior HR manager to take over from the incumbent.

30. The proactive approach to the change in HR personnel is good example of where POMS can be reassured by evidence of the AR recognising its obligations to the regulated entity and resolving issues promptly and with consultation. More examples of this level of consideration as matters arise in the course of business over the coming months will also be very welcome.

7

Recent FCA letters

31. The FCA have recently written to POMS (and many other connected firms) referencing the inquiry, and a reminder of the need for fit and proper personnel in both POMS and their AR. They also have reminded firms of their obligations to share any material information that might be of relevance to the FCA.
32. Both other principal firms have recently requested that POL inform them of anything they might need to share with the FCA, and POMS requests the same.
33. We have documented material examples of possible information that principal firms would want to be aware of to fulfil their disclosure obligations under the FCA Handbook Supervisory Principle 11. These include:
    a. POL as a legal entity is charged in respect of any criminal matter or is formally placed under investigation.
    b. Any Board Member of Member of Senior Management within POL are charged with a criminal offence or are notified formally that they are under investigation.
    c. POL becoming aware that any regulatory body has initiated an investigation or disciplinary proceedings against any Director or Senior Manager. This should include but not be limited to the Solicitors Regulation Authority (SRA), The Law Society of Scotland (LSS), The Institute of Chartered Accountants in England and Wales (CAEW) and the Institute of Chartered Accountants Scotland (ICAS).

Conclusion

34. The nature of an owner/regulated subsidiary/AR relationship is complex. Potential conflicts must be borne in mind, and care taken to ensure entities (and their governing bodies and management) are conscious of which capacity they are operating in when making decisions, the obligations that come with those capacities and that other entities may be impacted or considered during business matters.
35. POMS as a trading business is not generally operating at a high regulatory risk level. It is financially strong, has implemented the consumer duty regulations seriously and effectively, understands its risks and is governed well.
36. But the relationship with POL is a regulatory focus. It is an important arrangement and more complex (as owner and AR and service provider) than many principal/AR relationships and some aspects have required POMS management focus to improve.
37. A lot of good progress has been made. But with a focus on the new AR rules and the further heightened environment and interest generated by the inquiry, the FCA potentially has an even higher interest in POMS and POL than normal.
38. POMS had considered writing to POL to remind them of the matters outlined in this paper, and hopes that it, and the discussion at POL ARC, serves a useful purpose to ensure all parties are aware of the unusual, and potentially complex inter-entity relationship, and the need for POMS to be able to evidence effective oversight of its AR, notwithstanding its AR being its parent.

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

Title:	SPM Assurance Update	**Meeting Date:**	21 May 2024
Author:	Kelly Goodwin, Programme Director	**Sponsor:**	Chris Brocklesby, Group Transformation Officer

Input Sought: Noting

The Committee is asked to note the interim update, particularly:

- Work being undertaken to formalise the SPMP risk profile for current and future releases

1. Executive Summary

This paper is to provide the committee with details on the current status of work undertaken by SPMP since the last ARC update in February 2024 on identifying, assessing, and defining the key inherent risks and profiles for current and future releases.

As the Committee is aware, the programme successfully deployed Release 2.0 to Aldwych in February 2024. As well as the functionality previously available on R1, a subset of_Mails, Postage, Stamps and Mails admin journeys were added.

The programme deployed 2.1 to Aldwych, and subsequently to St Johns in Leeds. The plan is now to deploy Release 2.1 to Melville Road at the end of May 2024. By late summer SPMP plans to expand to 3 more DMBs and anticipate to 1 Non DMB by the end of 2024.

Since January 2024 the programme has been undertaking a number of key activities to ensure a great foundation exists to understand the risk profiles associated with SPMP and how these translate to our approach to releases:

- Draft Release / Deployment Strategy DMB vs Non DMBs
- Integrated Assurance & Risk Universe
- Mapping to past conformance requirements (WIP)
- IPA and Public Digital reports

Whilst we are not in a position to provide the ARC with a clear risk profile vs release, this paper identifies the next steps and timelines needed to achieve this.

2. Risk profile for current and future releases

As part of the Programme Business Case draft submission in March 2024, the programme developed a five-year technical roadmap overlaid by a deployment and release plan which provides clarity on the branch types for NBIT rollout through to 2028. This identifies 3 distinct phases:

- Pilot with DMB's
- Pilots including independent Postmaster branches / Strategic Partner branches
- Cutover branches to NBIT

In addition, over the last few months the programme has been preparing a deployment strategy which considers the optimal path to roll out the new platform across the POL footprint of 11199 branches[1].

[1] Number as at end March 2024 including outreach and excluding Drop & Collect.

Release / Deployment - Risk profile – WIP

In alignment with the Group ERM policy we will be developing the risk appetite and tolerance for a number of release / deployment scenarios, namely:

1) Pilot in Directly Managed Branches (DMB's)
2) Pilot in Independent/ Non-Directly Managed Branches (Non DMB's)
3) Full migration to Wave 1 (Simple local branches).
4) Full migration to all branches

The 4 scenarios provide the optimal balance between operational, legal and regulatory risks as these comprise risk to both the organisation and postmasters. We will be applying the following lens to our deployment / release profile to ensure all material inherent risks will be robustly assessed, monitored and tracked:

- Post Master Detriment, including platform integrity, is addressed as a part of the programme criteria
- Defects and backlog of defects are assessed at an individual and holistic aggregate level.
- Reputational Risk to the POL is considered.
- Hyper care/ Operational support processes and system are fit for purpose.
- Customer Experience is considered as part of the programme 'Go-Live'
- Ensure that system is operationally resilient to address legal and regulatory requirements and security risk

Please refer to ***Appendix 1*** *which provides a draft visualisation of how we will summate the risk appetite and tolerances.*

8

Initial pilots to DMBs will have limited impact if any problems were encountered due to dual running with Horizon. If any critical issues arise from NBIT, it can be switched off and colleagues will revert to using Horizon. The DMB risk profile has been reviewed by CISO and confirmed as low

Once Risk Tolerances have been agreed, a robust oversight and monitoring arrangements will be in place to ensure the deployments / releases continue to operate within risk thresholds. The governance applied will be :

- SEG – Responsible for Oversight
- RCC – Responsible for objective oversight and challenge – Sign off on risk appetite / tolerance and monitoring of exceptions.
- GE SPM Subcommittee – Accountable for assessment, monitoring and reporting of risks, including recommending risk exceptions and sign off's*

*Risk exceptions and sign off's will be subject to a formalised process including opinion sought from:

- Stakeholders impacted – Business, Banking partner etc
- Formal opinions from second line of defence (Group Assurance)
- RCC Sign off.

3. Next steps

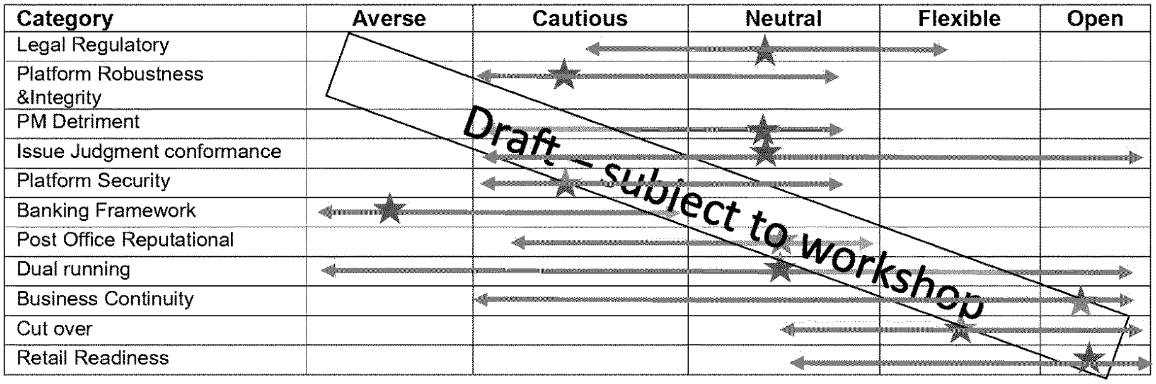
As mentioned above, we recognise this still does not provide a view to ARC on our risk profile, and therefore we have outlined below the key next steps and timelines we will be adhering to:

- Engage 3rd party specialist support to facilitate a risk workshop, to bring all key inputs and stakeholders to create the risk and appetite tables in **Appendix 1** for the various release / deployment scenarios – May 2024.
- Create and reach alignment within POL (program/business/stakeholders) on how the risk appetite and tolerance are to be operationalised i.e. the definition of each risk statements clearly quantified so that these can be then tracked and reported against by June 2024
- Embed clear risk exceptions and sign off's processes and procedures – June 2024
- Obtain RCC/ GE SPM Subcommittee approval for release / deployment risk appetite & tolerances – June 2024
- Update ARC – July 2024

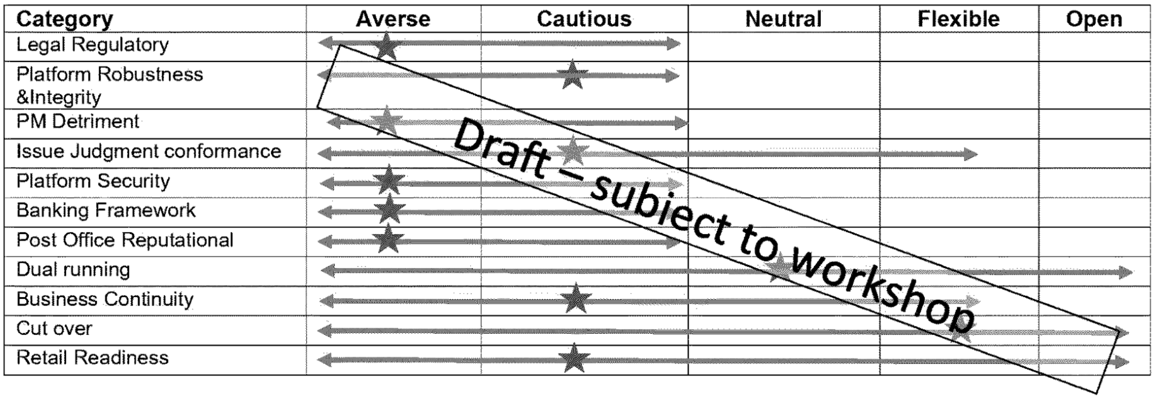
8

Appendix –
Risk Appetite ★ Risk Tolerance ←→

DMB Pilot



Non DMB (Independents) Pilot



8

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Cyber Update	**Meeting Date:**	21 May 2024
Author:	Neil Bennett, Chief Information Security Officer	**Sponsor:**	Chris Brocklesby, Chief Transformation Officer

Input Sought: Noting

Executive Summary

- Our Cyber operations continue to be effective in the face of increasing Global threats with no business impacting incidents in the reporting period
- IRRELEVANT
- The two strategic cyber risks remain outside of tolerance. The underpinning intermediate risks will be addressed through a combination of the Cyber Security Maturity Programme, other Technology Portfolio Programmes, and BAU activity.
- The Cyber Security Maturity Programme is on track to present the business case to POL Board in June
- A new CISO arrived on 18th March to lead the Cyber team, he will provide verbal observations to the committee

Report

1. Our Cyber Operations continue to provide effective defence against attacks despite a continued increase in the global threat.

2. Over the last month (March), our SOC successfully closed IRRELEVANT This is higher than normal due to additional monitoring that has been introduced on the AWS platform and a need to tune that monitoring. This additional monitoring is related to the NBIT production platform and is in direct response to a purple team exercise that was carried out in February which identified the priority use cases to be monitored.

3. No high severity incidents were logged in the month. IRRELEVANT IRRELEVANT

4. In February, we conducted two phishing exercises: a traditional password reset simulation and a more complex holiday policy change exercise. The results in terms of click through and reporting are shown below. The results indicate that our current approach IRRELEVANT IRRELEVANT

IRRELEVANT

5. All users who fail the exercise must complete phishing training on Success Factors, however, at the time of writing IRRELEVANT Discussions have commenced with HR to agree IRRELEVANT behaviours.

6. IRRELEVANT

9

IRRELEVANT

11.A new CISO joined the organisation on 18th March. Verbal observations will be provided to the committee.

Financial Impact

12.The total Cyber investment required for the maturity programme is expected to be IRRELEVANT

9

Next Steps & Timelines

13.Present business case to for phase 1 to SEG	20th May
14.Present Business case to POL Board	4th June
15.IADG Draw down for phase 1	18th June

POST OFFICE

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	IRRELEVANT	**Meeting Date:**	21 May 2024
Author:	Neil Bennett, Chief Information Security Officer	**Sponsor:**	Chris Brocklesby, Chief Transformation Officer

Input Sought: Noting

Executive Summary

IRRELEVANT

9

In response to the incident all impacted clients have been communicated with and a number of reviews were commissioned to ensure that the root causes are identified and truly understood and that remedial actions are implemented to ensure that the issue does not occur again. The immediate reviews were a Post Incident Review (PIR), an internal audit review of incident handling, and an independent external review of the changes made to access permissions in response to the incident. A further internal audit review is also underway with a wider remit but this will take longer to complete.

IRRELEVANT

A summary of the Internal Audit Review findings will be provided to ARC via a verbal update from Johann Appel, and the independent review of the changes made to access permissions is forecast to conclude on 9th May.

At the time of writing this paper further communication to clients was being prepared to appraise them of the PIR findings and resultant actions.

A further consideration that this incident prompts is the broader governance and oversight of our IT Controls Framework. A separate review will be conducted to assess this area.

The report contained in this paper is intended to provide the committee with a further level of detail on the incident, the causes and actions taken in response. It should be noted that whilst the cause of this specific incident has been remediated, until all actions have been completed there is still a risk of a similar incident occurring.

Report

What happened?

1. IRRELEVANT

9

2. Delays were experienced in the impact assessment of the incident by technical teams and although detail of the incident was emailed to the Data Protection team, proper process was not followed by technical support teams which resulted in delays to the incident being formally logged and subsequent delays in an initial assessment being performed from a Data Protection perspective.

3. IRRELEVANT

4. IRRELEVANT

What was the impact?

5. IRRELEVANT

IRRELEVANT

How did it happen?

IRRELEVANT

9

IRRELEVANT

9

How was it resolved?

IRRELEVANT

What is happening to ensure it doesn't happen again?

IRRELEVANT

9

17. A summary of the Internal Audit Review findings will be provided to ARC via a verbal update from Johann Appel, and the independent review of the changes made is forecast to complete on 9th May.

18. The full set of actions can be found in Appendix I.

19. A further consideration that this incident prompts is the broader governance and oversight of our IT Controls Framework. A separate review will be conducted to assess this area.

Financial Impact

20. The financial impact of this incident is currently not quantified.

Stakeholder Implications

IRRELEVANT

Next Steps & Timelines

24. The next steps are to proceed with the actions identified in each of the reviews. The full set of actions from the PIR can be found in Appendix I.

25. Delivery against actions will be tracked and overseen at the Technology Sub-Committee.

9

Appendix I

NB: At the time of writing this report work was still underway to determine assignees and due date for some actions.

Ref	Category	Action	Action Owner	Assigned to	Priority	Due Date	Status
PRB0042209 - 1	Process	Add SOC to the Service Now form, so the team are alerted once an incident is reported / elevated access requests to production is requested	Clare Mapes				Closed
PRB0042209 - 2	Process	Create an automated response to emails sent to the Data Protection Inbox and raise a ticket via Service Now for all potential data incident to prevent further issues being delayed	Clare Hammond				Closed
PRB0042209 - 3	Process	IRRELEVANT	Clare Hammond	Caoimhe McManus	High	31-May-24	Open
PRB0042209 - 4	People	Assess whether to provide additional data protection training to all new/existing NBIT resources	Clare Hammond	Caoimhe McManus	High	31-May-24	Open
PRB0042209 - 5	Process	IRRELEVANT	Paul Smith, Mark Nash, Clare Hammond	Caoimhe McManus	High	31-May-24	Open
PRB0042209 - 6	Process		Clare Hammond	Caoimhe McManus	High	31-May-24	Open
PRB0042209 - 7	Process		Mike Braithwaite		High	Jun-24	Open
PRB0042209 - 8	Process	Review and enhance the JML process for the programme	Mike Braithwaite		High	Jun-24	Open

PRB0042209 - 49	Process	Review the JML process with Service Operations before the process is rolled out into production	Mike Braithwaite		High	Jun-24	
PRB0042209 - 9	Process	Confirm if the JML process is within the IT control framework	Mike Braithwaite		High	Jun-24	Open
PRB0042209 - 10	Process	IRRELEVANT	Sophie Drury	Aaron Saunders			Open
PRB0042209 - 11	Process		Mike Braithwaite		High	Jul-24	Open
PRB0042209 - 50	Process		Mike Braithwaite		High	Jul-24	Open
PRB0042209 - 12	Process		Mike Braithwaite		Urgent	May-24	Open
PRB0042209 - 13	Process		Ben Owens				Open
PRB0042209 - 14	Tools		Ben Owens				Open
PRB0042209 - 15	Process		Ben Owens				Open

PRB0042209 - 16	Process	IRRELEVANT	Ben Owens				Open
PRB0042209 - 17	Governance	Identify old and outstanding risks that are stored outside of Service Now	Mike Braithwaite		High	May-24	Open
PRB0042209 - 18	Governance	Review the risk / impact and assign a new owner for all outstanding risks identified	Mike Braithwaite		High	Jun-24	Open
PRB0042209 - 19	Governance	IRRELEVANT	Mike Braithwaite		High	Jun-24	Open
PRB0042209 - 20	People	Provide training on the management of risks (SPM Engineers / People on the programme)	Mike Braithwaite		High	Jul-24	Open
PRB0042209 - 21	Governance	Ensure better governance and management of risk within the programme	Mike Braithwaite		High	Jul-24	Open
PRB0042209 - 22	Governance	Calculate our risks appetite against the Retail Deployment plan for non-functional requirements	Mike Braithwaite		Medium	Jul-24	Open
PRB0042209 - 23	Process	IRRELEVANT	Sophie Drury				Open
PRB0042209 - 24	Process		Graham Bevan	Jeff Burke	Low	31-May-2024	Open
PRB0042209 - 25	Process		Graham Bevan		Urgent		Close

PRB0042209 - 26	Process	Complete a mapping exercise between AIS and the HLD to validate that we have created documentation to the right design specification.	Graham Bevan	Jeff Burke	Low		Closed
PRB0042209 - 27	People	IRRELEVANT	Mike Braithwaite		Urgent	Apr-24	Open
PRB0042209 - 28	Process	Create a BAU process for maintenance of the data flow documentation (to ensure a single source of truth is available at all times).	Graham Bevan	Jeff Burke	Low	31-May-2024	Open
PRB0042209 - 29	Process	IRRELEVANT	Graham Bevan	Richard N Cater	Low	31-May-2024	Open
PRB0042209 - 30	Process		Graham Bevan		High		Closed
PRB0042209 - 31	Process		Graham Bevan		Low		Closed
PRB0042209 - 32	People		Clare Hammond		Medium		Open
PRB0042209 - 33	Process		Graham Bevan	Cliff Concious	High	Oct-24	Open
PRB0042209 - 51	Process		Sophie Drury		Urgent	Jun-24	Open

PRB0042209 - 34	Governance	IRRELEVANT	Mike Braithwaite		High	Oct-24	Open
PRB0042209 - 35	Process	Get external verification that the initial fix activities are sufficient to prevent a reoccurrence of this issue.	Mike Braithwaite		Urgent	Apr-24	Open
PRB0042209 - 36	Governance	IRRELEVANT	Mike Braithwaite		Medium	Oct-24	Open
PRB0042209 - 37	Process		Graham Bevan	Richard N Cater	High	01-May-2024	Open
PRB0042209 - 38	Process		Graham Bevan	Richard N Cater	High	01-May-2024	Open
PRB0042209 - 39	Process		Rob Wilkins		Medium		Open
PRB0042209 - 40	Process		Clare Hammond	Graham Bevan	High		Open
PRB0042209 - 41	Governance		Rob Wilkins		High		Open
PRB0042209 - 42	Process		Rob Wilkins		Medium		Open
PRB0042209 - 43	Process		Rob Wilkins		High		Open
PRB0042209 - 44	Process	Conduct a review between architectural design and what has actually put in place for NBIT	Ben Owens				Open
PRB0042209 - 45	Process	Create Low Level designs for new services and architectural changes	Ben Owens				Open
PRB0042209 - 46	Process	Create an assurance process between requirements, architectural design and architectural delivery	Ben Owens				Open

PRB0042209 - 47	Governance	Discuss programme governance and prioritization of functional and non-functional delivery	Mike Braithwaite		High	Apr-24	Open
PRB0042209 - 48	Process	Review the prioritisation of technical debt / remediation within the programme	Mike Braithwaite		High	Apr-24	Open

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Taskforce on Climate related Financial Disclosures (TCFD) and ESG Journey.	**Meeting Date:**	21st May 2024
Author:	Mark Cazaly – Head of Corporate Responsibility. Martin Hopcroft – Director of Health, Safety, Environment and Business Continuity.	**Sponsor:**	Kathryn Sherratt – Interim Chief Finance Officer

Input Sought: Noting

The Committee is asked to **note** the approach to TCFD, with quarterly updates provided to RCC.

Executive Summary

The UK Government has set requirements through the Companies (Strategic Report) (Climate-related Financial Disclosure) Regulations 2022 that companies and limited liability partnerships (LLPs) with more than 500 employees and a turnover of more than £500m must report a 'Non-Financial and Sustainability Information Statement' (NFSIS) in line with the recommendations of the TCFD. Companies and LLPs are encouraged to embrace the 'spirit' of the regulations, not just the letter, by truly embedding climate-change considerations into all aspects of managing a business.

Businesses within scope will be required to include disclosures on climate change-related risks and opportunities, where these are material. The disclosures should cover how climate change is addressed in corporate governance; the impacts on strategy; how climate-related risks and opportunities are managed; and the performance measures and targets applied in managing these issues. As a company with more than 500 employees and a turnover of more than £500m, Post Office must report in line with these requirements for FY 2023/24 – this has been confirmed by our auditors, PwC. Much of the content and processes for the report are already covered by our overall risk management approach and we have recently added four climate-specific risks to the risk register to expand our coverage in this area, along with appetite statements which have been included in the latest risk paper for approval.

10

In order to provide a Non-Financial and Sustainability Information Statement, we will work with our existing supplier, Inspired Plc, which already supports our Streamlined Energy and Carbon Reporting (SECR) for our ARA.

This will require Board sign-off as part of our ARA and we must be able to highlight that the appropriate governance is in place to show that climate risks and opportunities are being considered by the Board – this will be done through the RCC quarterly and through the ARC annually.

Report

Climate Action and Carbon Reduction

1. With the legal requirement that all UK business are Net Zero by 2050, POL should begin to set out a roadmap for achieving this goal, or even going further by implementing Net Zero earlier. Many key partners and clients such as Royal Mail, Bank of Ireland, Amazon and Tesco have already set Net Zero dates; WH Smith have even set a Scope 3 Net Zero target for 2040 – this means a decarbonised supply chain, including Post Office. For many of our financial services partners, they will also be captured by the FCA's regulations around climate reporting and as a supplier, will be expecting POL to provide them with information to inform their own reporting – we are already seeing this with emissions data with a number of banking clients requesting our emissions data – we can expect further queries around our climate strategy as they build out the scrutiny of their supply chain.

2. There is a significant amount of work to do to put ourselves on a credible trajectory to meet the 2050 deadline. Over 2024/25 we will build our capability and maturity on issues around Net Zero beginning more formal work such as setting science-based targets. Getting to Net Zero is likely to require significant investment in due course.

<u>Carbon Reduction Plan</u>

3. We are building our capability around Net Zero by working with existing suppliers such as OCS (FM Service Supplier) and Inspired Plc, and there are a number of significant actions we can take to improve our environmental credentials;

- Reducing Water and Energy Usage across our estate, energy efficient technologies and education to encourage responsible behaviour.
- Reducing Transport Emissions – clear roadmap to switch to a low carbon fleet, commercial (red fleet) and company cars to EV (Electric vehicles).
- Business Travel – reduce impact of business travel by educating colleagues and sharing trip CO2 emission data, encouraging responsible 'method of travel' choices.
- Facilities Management e.g. reduce waste and single use plastic.

10

4. Conclusion from **Internal Audit** (22/23) of Readiness to report TCFD from the 23/24 ARA.
   a) POL has been reporting under Streamlined Energy & Carbon Reporting legislation, in its Annual Reports & Account for the past three years. For the financial year 23/24, there is a requirement to also report under the Taskforce on Climate-related Financial Disclosures.

   b) There are sufficient mitigations to assess, manage, and disclose ESG positions and associated risks. However, the alignment of ESG goals, targets, and strategy with Post Office strategy/priorities is work in progress.

   c) We confirm that there is readiness for ESG reporting under the Taskforce on Climate-related Financial Disclosures with sufficient planning in place to assess, manage, and disclose ESG positions and associated risks. Whilst it is not mandatory to disclose Scope 1, Scope 2 and Scope 3 greenhouse emissions under the climate-related Financial Disclosure regulations for UK, it is required under the SECR legislation, and the data currently being reported is sufficient.

Climate-Related Scenarios

5. One of the Taskforce's key recommended disclosures focuses on the resilience of an organisation's strategy, taking into consideration different climate-related scenarios, including a 2° Celsius or lower scenario. An organisation's disclosure of how its strategies might change to address potential climate-related risks and opportunities is a key step to better understanding the potential implications of climate change on the organisation. The Taskforce recognises the use of scenarios in assessing climate-related issues and their potential financial implications is relatively recent and practices will evolve over time, but believes such analysis is important for improving the disclosure of decision-useful, climate-related financial information.

6. Post Office will need to undertake an analysis of how different climate change scenarios will impact the business and the mitigations the business will need to implement. This will require the support from an external third party.

TCFD recommendations and UK government implementation

7. Recognising that climate-related financial reporting is still evolving, the Taskforce's recommendations provide a foundation to improve stakeholder's ability to appropriately assess and price climate-related risk and opportunities. The Taskforce's recommendations aim to be ambitious, but also practical for near-term adoption. The Taskforce expects to advance the quality of mainstream financial disclosures related to the potential effects of climate change on organisations today and in the future and to increase shareholder engagement with boards and senior management on climate-related issues.

8. Improving the quality of climate-related financial disclosures begins with organisations' willingness to adopt the Taskforce's recommendations. Those organisations in early stages of evaluating the impact of climate change on their businesses and strategies can begin by disclosing climate-related issues as they relate to governance, strategy, and risk management practices. The Taskforce recognises the challenges associated with measuring the impact of climate change, but believes that by moving climate-related issues into mainstream annual financial filings, practices and techniques will evolve more rapidly.

10

9. The UK government's implementation of the TCFD recommendations means that companies and LLPs are both required to disclose the following information:

(a) a description of the governance arrangements of the company or LLP in relation to assessing and managing climate-related risks and opportunities;

(b) a description of how the company or LLP identifies, assesses, and manages climate related risks and opportunities;

(c) a description of how processes for identifying, assessing, and managing climate-related risks are integrated into the overall risk management process in the company or LLP;

(d) a description of—

(i) the principal climate-related risks and opportunities arising in connection with the operations of the company or LLP, and
(ii) the time periods by reference to which those risks and opportunities are assessed;

(e) a description of the actual and potential impacts of the principal climate-related risks and opportunities on the business model and strategy of the company or LLP;

(f) an analysis of the resilience of the business model and strategy of the company or LLP, taking into consideration of different climate-related scenarios;

(g) a description of the targets used by the company or LLPs to manage climate-related risks and to realise climate-related opportunities and of performance against those targets; and

(h) the key performance indicators used to assess progress against targets used to manage climate-related risks and realise climate-related opportunities and a description of the calculations on which those key performance indicators are based.

10. POL will be required to report in line with the points above in the Non-Financial and Sustainability Information Statement.

Considerations and Next Steps

Service 1. TCFD Compliance Statement 2023/24

11. The TCFD Compliance Statement disclosure service provided by Inspired Plc is a compilation of information required to align with the TCFD framework of eleven disclosures, each representing an element of governance, risk management, strategy, and metrics and targets within POL. Inspired will produce a comprehensive compliance statement, detailing efforts undertaken by POL through the reporting year, and actions identified to be completed in future reporting years to ensure full compliance with its government reporting requirements. This compliance statement will cover the four key themes of the disclosure: Governance, Strategy, Risk Management and Metrics and Targets. (See Appendix A).

10

Service 2. TCFD Workstreams 1 – 8. 2024/25

- Climate – Related Governance

12. Stakeholders are interested in understanding the Board's role in overseeing climate-related issues and how management is assessing and managing those issues. Inspired Plc's services will build capacity with the Board to enable them to consider climate-related issues better when reviewing the business strategy and operations. The services will support the development of practical management processes to monitor and report on climate-related matters. The climate-related governance deliverables include: Board of Directors capacity building session. Project updates for Board, Committee and SteerCo packs and attend some meetings, if required.

- Climate Scenario Modelling and Risk Management Framework

13. Climate scenario analysis is a tool that can inform POL's strategy and financial planning. Scenarios are hypothetical constructs that provide a way for organisations to consider how

the future might look if specific trends continue or certain conditions are met. The tool will enable POL to evaluate its operational resilience to climate change utilising three warming pathways over three 'time horizons'. All risks and opportunities are considered in relation to the appropriate sector and/or geography. The analysis is delivered to key stakeholders in the climate risk and opportunity workshop.

- Climate Risk and Opportunity Workshops

14. The analysis from the scenario modelling and risk assessment is delivered to key stakeholders in the climate risk and opportunity workshop. The two-hour interactive workshop is an essential step in building a comprehensive climate risk and opportunity register. The climate scenario modelling and risk management framework deliverables include climate risk and opportunity workshop materials. It is recommended that the Board participate in this session.

GHG Emissions Workstreams

- Scope 1 and 2 emissions calculations.
- SECR Compliance – Carbon consumption and emissions report and efficiency implementations and methodology.
- Carbon Balance Sheet - POL's Greenhouse Gas (GHG) emissions metrics and targets. Metrics and Targets are used to assess the organisation's climate-related governance, progress against strategic objectives, and management of climate-related issues.
- Net Zero Strategy Emissions Modelling and Net Zero Strategy Report.
- Net Zero Workshop and materials.

TCFD Deliverables

- Fully branded TCFD Report to communicate to stakeholders how POL is responding to climate-related risks and opportunities.
- Fully branded TCFD Index to provide a simple overview of progress.
- TCFD Annual Report Disclosure ensuring POL complies with its government and FRC reporting requirements.

10

Financial Impact

15. Costs of the reporting. £60k + VAT / annum. 23/24 Statement and Q1 report have been covered under the current OCS contract. Q2 – Q4 (24/25) contract to be procured and funding identified. Inspired PLC have provided us with a cost proposal and ESG framework.

Risk Assessment, Mitigations & Legal Implications

16. We are obliged to publish annual SECR and TCFD reports in our Annual Report and Accounts. In order to be compliant we must evidence Board oversight, governance and strategy, risk assessment and targets and metrics. Failure to do this would leave us in breach of the TCFD Regs 2022 from 24/25.

Stakeholder Implications

17. Internal – resource will be required from existing colleagues, primarily through the Environment and Sustainability Support Group including H&S and Environment, Property,

Fleet, Supply Chain, Procurement, Business Continuity, Corporate Affairs, Strategy and Transformation and Contract Managers

18. External – this will help us satisfy regulatory reporting requirements and provide comfort to key clients around our approach to climate risk.

Appendix

<u>Further background on TCFD requirements</u>

Climate change affects all entities to a greater or lesser extent and presents both risks and opportunities to businesses. Climate-related reporting focusses on the way in which climate-related risks and opportunities are identified, assessed, managed, and reviewed. Reporting on climate-related matters needs to be proportionate to the way in which each business is affected – one size does not fit all.

In the UK, the Financial Conduct Authority and UK Government have set us on a path to mandatory reporting. The UK Government is making TCFD-aligned disclosure mandatory for over, 1,300 of the largest UK-registered companies and financial institutions; making it the first G20 country to do so. The objective of the regulations The Companies (Strategic Report) (Climate-related Financial Disclosure) Regulations 2022 have been introduced in the UK to help support informed investor decisions as the UK progresses towards a low-carbon economy. The regulations state that Companies and LLPs with more than 500 employees and a turnover of more than £500m must report in line with the recommendations of the TCFD. Companies and LLPs are encouraged to embrace the 'spirit' of the regulations, not just the letter, by truly embedding climate-change considerations into all aspects of managing a business. Companies and LLPs within scope will be required to include disclosures on climate change-related risks and opportunities, where these are material. The disclosures should cover how climate change is addressed in corporate governance; the impacts on strategy; how climate-related risks and opportunities are managed; and the performance measures and targets applied in managing these issues. (See Appendix). Given Post Office' position as an arms-length body, POL is in scope for reporting in line with these requirements.

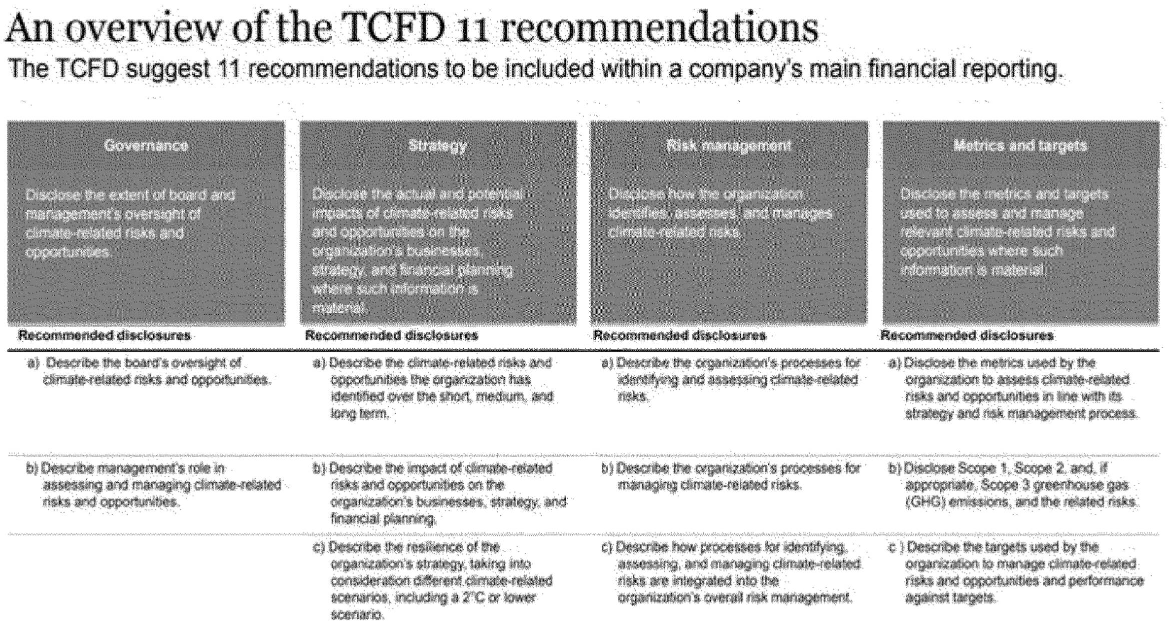
10

A comprehensive TCFD report enables Post Office to clearly demonstrate to its stakeholders, including UKGI, that it is taking the issue of climate change seriously. The workstreams that support the annual preparation of the TCFD report will help Post Office develop the necessary internal processes and streamline its reporting requirements. Apart from the government compliance requirement, a TCFD report is an excellent way of communicating with stakeholders at a time when society is seeking more sustainable operating solutions. The disclosure will help establish that POL is a robust asset for the government.

POL has worked with Inspired PLC for mandatory compliance solutions for SECR (Streamlined and Carbon Reporting Scheme) since inception in 2019. They will support Post Office to produce an effective and impactful annual Taskforce on Climate-Related Financial Disclosure (TCFD) Statement for the 23/24 Annual Report and Accounts and subsequent TCFD quarterly reports for RCC and ARC, commencing Q1 24/25.

ESG is a journey and the disclosures evolve over time as the company develops its ESG strategy and competency. Whilst Inspired PLC are contracted via the FM service supplier, OCS, to produce the initial TCFD statement for 23/24 and the Q1 (24/25) Report, POL are seeking to engage a single partner that can provide all of the services and in addition, provide strong support on delivering an actionable transition plan to net zero. Commencing Q1, Inspired PLC will work with stakeholders to assess Post Office's entire value chain against the TCFD disclosure recommendations. The identified gaps and areas of development will inform the workstreams' next steps. Inspired PLC will also provide workshops with key stakeholders to build climate-related capacity within Post Office e.g. climate-risk and opportunity workshop. Inspired PLC's 'delivery' aims to build ESG knowledge from a data perspective and work with Post Office to improve data collection and quality. They will produce a 'compliance statement' for the purposes of compliance with the government's Climate-Related Financial Disclosure requirements, detailing efforts undertaken and planned for the future for mitigation of Post Office's ecological footprint. Inspired PLC will also continue the production of a full Streamlined Energy and Carbon Reporting disclosure for Post Office, detailing annual operational emissions for the reporting year. This disclosure will also support the compliance statement narrative within the theme of Metrics and Targets. (See Report and Appendix for TCFD Framework).

SEG Sponsorship for Post Office ESG is shared between the CFO and Corporate Affairs Director. The Director of H&S, Env and Business Continuity has responsibility for the Environmental and Sustainability Policies and is supported by stakeholders who are members of an Environmental and Sustainability Working Group (ESSG - Heads of CSR, Property, Fleet, Supply Chain, Risk, Business Continuity, Procurement and Strategy and Transformation). This group ensures data is supplied to our supplier, Inspired PLC, who undertakes data validation and produces compliant reports for the ARA. The group will work closely with Inspired PLC to undertake a climate scenario modelling and analysis during 24/25 to help identify risks and impacts on financial disclosures. Quarterly reports will be produced for RCC and ARC to review risk and impact, and Board will be sighted to ensure climate risk and opportunities are considered in strategic thinking and planning.



An overview of the TCFD 11 recommendations

The TCFD suggest 11 recommendations to be included within a company's main financial reporting.

Governance	Strategy	Risk management	Metrics and targets
Disclose the extent of board and management's oversight of climate-related risks and opportunities.	Disclose the actual and potential impacts of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning where such information is material.	Disclose how the organization identifies, assesses, and manages climate-related risks.	Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material.
Recommended disclosures	**Recommended disclosures**	**Recommended disclosures**	**Recommended disclosures**
a) Describe the board's oversight of climate-related risks and opportunities.	a) Describe the climate-related risks and opportunities the organization has identified over the short, medium, and long term.	a) Describe the organization's processes for identifying and assessing climate-related risks.	a) Disclose the metrics used by the organization to assess climate-related risks and opportunities in line with its strategy and risk management process.
b) Describe management's role in assessing and managing climate-related risks and opportunities.	b) Describe the impact of climate-related risks and opportunities on the organization's businesses, strategy, and financial planning.	b) Describe the organization's processes for managing climate-related risks.	b) Disclose Scope 1, Scope 2, and, if appropriate, Scope 3 greenhouse gas (GHG) emissions, and the related risks.
	c) Describe the resilience of the organization's strategy, taking into consideration different climate-related scenarios, including a 2°C or lower scenario.	c) Describe how processes for identifying, assessing, and managing climate-related risks are integrated into the organization's overall risk management.	c) Describe the targets used by the organization to manage climate-related risks and opportunities and performance against targets.

10

POST OFFICE

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Banking Deep Dive	**Meeting Date:**	21 May 2024
Author:	Ross Borkett	**Sponsor:**	Owen Woodley

Input Sought: Noting

ARC has requested a bi-annual deep dive into Banking and the Committee is asked to note the contents of the report.

Executive Summary

This paper provides a deep dive into specific banking risks for consideration and noting by the Committee, covering:

- Access to Cash legislation
- Banking Framework 4
- Deposit Limits and Anti-Money Laundering
- IRRELEVANT
- PWC audit

Access to Cash legislation has now passed through parliament and into law. The FCA has consulted with the industry and the new rules will be published in July 2024 and be live by September 2024. This brings new obligations on the banks to provide access and new information gathering powers over the Post Office for the services we offer.

We are in the middle of BF4 negotiations with the banks to secure a continuation of IRRELEVANT Negotiations will continue through the coming months.

Money laundering remains a significant risk for the business – the National Economic Crime Centre believe we are still being targeted by criminals. Deposit limits have now been implemented and improved controls at the banks are believed to be creating more "friction" to deter criminals, but it remains an ongoing challenge to manage and mitigate in partnership with the banks.

In the last year the banking service has experienced disruption through the underperformance of a supplier called IRRELEVANT These outages are causing issues for customers and the banks and IRRELEVANT at a IRRELEVANT IRRELEVANT Senior IT leaders are engaged in escalations but our leverage to resolve these issues is poor. Further fixes are being implemented in the coming months to reduce the impact of further outages.

Report

Access to Cash Legislation

1. Access to Cash legislation was part of the Financial Services and Markets bill that passed into law last year. The FCA consulted on new regulations in January 2024 and are expected to publish the new rules in July 2024, with implementation by September 2024.

2. The legislation places obligations on the largest financial institutions to provide access to withdrawal and deposit services, with the FCA gaining new powers to regulate for this. This will be set out as a minimum geographical access criterion, similar to the access criteria Post Office has with UKGI, for cash withdrawal and deposit services, with Great Britain and Northern Ireland being treated separately recognising the different banking environment across those regions. The consultation on the new rules suggested that banks are expected to assess local needs for cash, for example if there is a need for an assisted service or extended hours. They are not defining a single, nationwide standard to be met. This allows banks to adapt the provision over time as cash declines.

3. HMT are expected to announce which firms are "designated" in June 2024. This will certainly include the largest financial institutions but may stretch into some of the medium sized and regional banks too, including those in Northern Ireland. It is unclear if Nationwide will be caught or not.

4. LINK will be regulated by the FCA for this too in their role as the coordinator for cash solutions (deciding if a community needs a banking hub or deposit solution).

5. Cash Access UK (the banks' delivery company) believe they will escape direct regulation.

6. The FCA will gain information gathering powers over the Post Office. They have shared their initial requirements with us, and we are reviewing these internally. We have recruited a new role, Head of Access to Cash, who's priority is to coordinate our response to these information gathering requests. This will provide the FCA and industry with much more visibility of changes to our network (closures, openings, etc).

7. Some banks have not responded well to the FCA consultation. They believe that the FCA have over-regulated compared to the original Treasury policy statement. They believe the FCA's approach will create a greater demand for interventions to provide access to cash and are threatening the FCA with further bank closures to cover the cost. We don't anticipate the FCA to change their rules materially from the consultation.

Banking Framework 4

8. Our current agreement with the banks, Banking Framework 3, IRRELEVANT We commenced negotiations with the banks in IRRELEVANT and aimed to present our final offer to the banks in IRRELEVANT. However, IRRELEVANT IRRELEVANT Subject to agreement, these negotiations are expected to continue through to IRRELEVANT with

final POL Board governance sign off in IRRELEVANT r. Banks will then have until IRRELEVANT to sign up to the deal.

9. IRRELEVANT

10. We are using IRRELEVANT deal for BF4, rather than IRRELEVANT This IRRELEVANT

11. The deal provides IRRELEVANT BF4 will IRRELEVANT IRRELEVANT

12. There IRRELEVANT IRRELEVANT For example, IRRELEVANT IRRELEVANT On the first of these, we should expect the industry to test alternative solutions to use, IRRELEVANT We've assumed IRRELEVANT but aim IRRELEVANT IRRELEVANT

13. IRRELEVANT

Deposit Limits and Money Laundering

14. The FCA have put significant pressure on financial institutions to strengthen their money laundering controls to combat growing concern over financial crime. This follows some banks being fined significant financial penalties over the last 2 years for previous failings.

15. With bank branch networks continuing to be rationalised, there is a greater reliance on the Post Office network for cash deposits. Over the last year we have performed over £2bn in cash deposits every month, supporting personal and business customers with their cash needs. In this role we are underpinning the cash system and are aligned to the Government's aims to protect access to cash.

16. However, there are concerns that with such a heavy reliance on our network for deposits, and with Postmasters having less information available at the counter than in a bank branch, that criminals are targeting our network. The National Economic Crime Centre still believe that criminals are laundering hundreds of millions through the Post Office network annually.

11

17. In response to this, the FCA has put pressure on banks to implement deposit limits on transactions through our network. This has resulted in banks implementing various limits over the last 2 years to attempt to reduce the impact.

18. These limits have acted as a blunt instrument and have had an impact on legitimate customers trying to deposit. We have made numerous interventions and escalations over the last 2 years to get the balance right between access to cash and reducing money laundering. This has achieved some changes to limits and a more sensible approach from those who implemented later. The FCA has closely reviewed the impact and generally believes the banks have achieved the right balance but encourages them to continue to review them over time. All banks have now implemented limits and there are no expectations they will be removed.

19. Our view remains that these limits will not have a significant impact in reducing financial crime as criminals will simply use multiple accounts to deposit, making it harder to detect. Evidence from the last year suggests this is the case. However, the FCA are representing the significant implementation of limits as a successful intervention and intend to close this programme of activity – moving back to BAU interactions with us on AML. Their next focus will be on deposits through the PayPoint network.

20. There is a reluctant acceptance of these limits by Postmasters and customers. It remains a topic that is raised when visiting with Postmasters but is no longer something we receive proactive complaints about. We have made efforts to improve the customer experience through the inclusion of limits on Horizon Help, and the introduction of a receipt message detailing how much a customer has left of their limit (only a subset of banks has implemented this to date). Both interventions have been received positively.

21. The industry continues to face challenges over money laundering and until greater coordination between banks it is hard to see material improvements. This includes the need for easier information sharing between banks to identify customers who are using multiple accounts, improved monitoring, detection, and looking at customer account behaviour (for example, looking at where customers deposit and immediately move the money out of the account). The Home Office is imminently announcing some changes that may aid information sharing.

11

22. We will continue to collaborate with the industry in mitigating this issue as our role in deposits continues to grow. This could, for example, include further checking of ID as part of the transaction.

Worldline Service Issues – Risk 0022230

23. Since April 2022 there have been a number of incidents connected to the banking services infrastructure where the Worldline interface has been subject to an outage / issue. The main focus of the risk are instances associated with the processing of bank customers whereby withdrawals / deposits have been declined on Horizon, however the debits and or credits have reached the customers bank accounts - e.g. withdrawals have been

declined, the customer has not been given the money but their account has been debited / deposits have been declined, the customer has not handed over the funds but their account has been credited. It is not a Horizon issue.

24. These failures result in differences in the settlement files whereby the Post Office has to pay banks funds to recredit their customers' accounts and work with banks to attempt to recall finds deposited in error in their customers' accounts. All losses sit at POL level, there is no impact on Postmasters accounts. The impact on the banks under Banking Framework is they have to manually work all erroneous transactions, contacting all impacted customers therefore taking up time and resource within the banks. This also impacts customers and could have real impact on their ability to manage their finances, miss key financial commitments and lead to distress and potentially financial hardship particularly concerning withdrawals. These issues lead to poor customer outcomes.
25. Since May 2023 these instances have significantly increased, 12 instances of outages with 7 different root causes. 3 of these instances led to significant volumes for banks to correct, May 2023 - 1,053, November - 733 and February 2024 - 539. To date £89.4k has been written off and £41k has been provisioned for the latest February incident.
26. A number of fixes have been deployed by Worldline to address the failures in the system with 3 further fixes in the process of being tested / built and scheduled for deployment. This includes a service from Vocalink that should reduce the amount of manual work needed by banks and establish an auto reversal mechanism. The cost of this to POL is circa £356,000.
27. The issues have been escalated within POL and several conversations have taken place with senior executives within Fujitsu and Worldline. This is complicated as Worldline are a subcontractor of Fujitsu, therefore POL does not have a direct contractual relationship with Worldline. POL also faces the challenge that the volumes of transactions impacted are very low from a Worldline / banking transactions perspective and only classed at low level incidents. They do not take account of the customer / POL reputational risks / impact.
28. As well as the financial risk, banks are now asking for contributions to the distress and inconvenience payments they are making to their customers (£50 for withdrawals), it is having a significant reputational risk between POL and the Banking Framework participants. The major banks have escalated this internally and we are seeing these concerns play out in Banking Framework 4 negotiations. Most banks have little, or no confidence POL is able to provide a sufficiently robust banking services platform.
29. Next year there may be an opportunity to move the Worldline contract to a direct agreement with POL. Senior IT leadership are engaged in escalations, but we remain at risk until these latest fixes are implemented.

11

PWC Audit of the Banking Framework

30. In 2022 5 institutions in the Banking Framework exercised their right under Clause 15 of the Banking Framework agreement to appoint an external auditor to perform an assurance audit of Post Office's compliance with Banking Framework 2.3. Banks could not agree who (amongst them) should lead, and PWC stated that they would not work with a 'group of banks' therefore we were asked, and we agreed, to be the lead organisation, giving us the opportunity to review any output before any banks. PWC were appointed to undertake this work, and started the audit on the 1st August with the final report delivered March 2023.

31. IRRELEVANT Management actions were agreed and have been progressed since March 2023 to complete the management actions.

32. IRRELEVANT tracking the completion of them in their risk committees and require POL to provide evidence, including senior business owner sign off, the actions have been successfully delivered by

33. IRRELEVANT

Stakeholder Implications

34. IRRELEVANT

35. Access to Cash regulations will require Post Office to provide far greater insight of our network to the industry, including accurate opening hours, accessibility features, and details of any temporary and permanent closures. This will require us to improve the robustness and integrity of our data. This is an activity we are progressing with the relevant data teams.

11

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Procurement Risk & Compliance Report	**Meeting Date:**	21 May 2024
Author:	Lian Carroll - Procurement Director	**Sponsor:**	Kathryn Sherratt, Interim Group Chief Finance Officer

Input Sought: Noting

The Committee is asked to review the report, noting the Procurement Risk Exceptions submitted to the Post Office Strategic Executive Group or Board since March 2024. A visual breakdown of all Open incidents as of 1 May 2024 is available in Appendix A.

Executive Summary

Since the last ARC report in March 2024 there have been no Procurement Risk Exceptions submitted to the Strategic Executive Group or Board for approval. All existing risks as detailed in Appendix A have previously been agreed with Board. Our overall non-compliance value has IRRELEVANT This is due to bringing the contract with CACI into compliance via POL's software reseller contract with SCC.

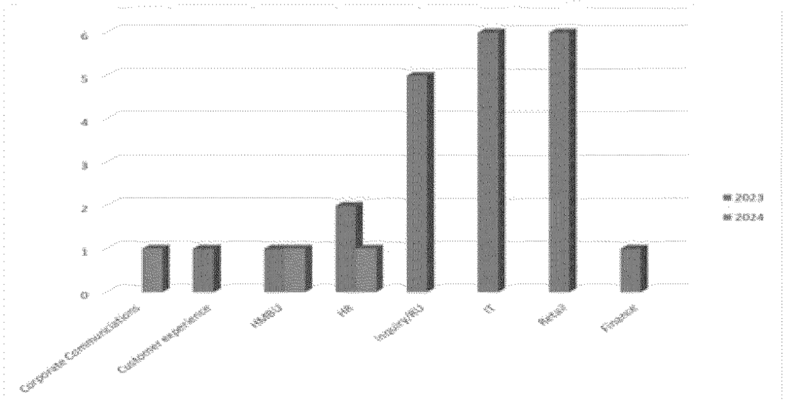
There are a number of issues with the data quality of contracts held in the Web3 system which may lead to the discovery of further non-compliance.

Report

Across the Group Post Offices operates a decentralised contract management model whereby individuals across the business are responsible for managing relationships between Post Office, vendors, and the respective contracts. This model was approved at ARC in September 2020 being considered more cost efficient and less disruptive than creating a centralised contract management team.

In 2021 a previous report to RCC and ARC highlighted the continuing issues with the adoption and embedding of the management of contracts across the business. Several improvements in training and reporting were implemented including the establishment of a centralised contract admin centre for revenue contracts. Despite the previous work undertaken to address the aspects highlighted in 2021 we are still seeing significant compliance issues in the adoption of the Contract Management Framework for cost contracts.

As a proxy measure for contract management failure we are monitoring the use of Regs 72, contract modifications and Reg 32 direct awards and as can be seen in the graph below there were 22 in FY 2023 and 3 so far in FY 2024.



To ensure compliance and mitigate the risks associated with poor contract management including data integrity and the challenges of embedding the Contract Management Framework in the business SEG is now looking at organisational design options together with changes in the approach to contract management across the group.

Next Steps

Recommendations on how to address and resolve the issues highlighted in the report above should be agreed by SEG before being taken to ARC for discussion and approval.

12

Appendix A - All Open Material Incidents

IRRELEVANT

£143,920,000

IRRELEVANT and Camelot Cheques. IRRELEVANT

IRRELEVANT

Payment Services – Board approved a direct award in November 2022. Zunoma (previously Smith & Ouzman), have been operating as POL's security print provider since the commencement of Payouts in 2006. The original contract was created in June 2018 and backdated to 2015. The contract expired in July 2019. The Energy Payouts were put through the Zunoma contract as this was seen by the Business as a continuation of a BAU service. The direct award of the contract to Zunoma is non-compliant with the Public Contract Regulations. It is Procurement's view that we are unlikely to receive a challenge to this direct award.

HSF - In June 2019, a Non-PCR Compliant Direct Award was made to HSF to advise POL on [redacted] The Board did however consider PCR 2015 compliance in 2021 when a decision to appoint HSF as POL's legal representative at the Inquiry was made via a further Non-PCR Compliant Direct Award. With respect to the Inquiry, Group General Counsel set out the following options to Board in 2021: [redacted]

12

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Postmaster Support Policies – Annual Review	**Meeting Date:**	21st May 2024
Author(s):	Jo Milton, Senior Process Improvement Manager	**Sponsor:**	Martin Roberts, Group Chief Retail Officer

Input Sought: Approval

The Committee is asked to approve three updated postmaster support policies to be effective from the date of approval:

- Postmaster Complaint Handling
- Network Monitoring and Branch Assurance Support Policy
- Network Cash and Stock Management Policy

Executive Summary

Following the Group Litigation Order (GLO), Post Office created a suite of postmaster support policies, all of which were initially approved by ARC in 2021 and have been in use since.

The purposes of these internal policies are to provide guidance, set down principles and highlight risk areas, while also ensuring that Post Office can support postmasters effectively and compliantly with the GLO.

In March 2022, ARC agreed that annual reviews should continue to take place, on a phased basis.

The policies submitted here were last approved at ARC in December 2022 (Complaint Handling and Network Monitoring and Branch Assurance) and January 2023 (Network Cash and Stock Management).

Report

Policy Assurance Review Work

1. Specific feedback from the internal policy assurance reviews completed by the Group Assurance team have been incorporated, where applicable, into these policies. The Assurance review highlighted a number of actions, and a brief summary of progress against these actions is included under each policy heading below.

2. In addition, a review of risks and controls within our suite of Postmaster policies has been completed for these three policies, following guidance from Group Assurance. The rest will be completed by the end of July.

13

Overview of changes made

3. General updates have been made to the policies, since the last approval:
   a) Risks and Policy Required Operational Standards have been updated and reflect those managed and monitored on ServiceNow for consistency.
   b) Policy owners have been updated following a decision for all policies to be owned by the Retail Engagement Director, on behalf of Retail.
   c) Wording has been updated to reflect what happens if a risk sits outside the agreed Risk Appetite/Risk Tolerance level (this has been agreed with the Head of Risk).
   d) Contact details for the National Federation of Sub-Postmasters have been added.
   e) Name of the Postmaster Decision Review policy changed to Postmaster Contract Termination Decision Review policy.

4. A list of more specific and minor updates in each policy are set out in Appendix 7, but the main changes are summarised below:

Postmaster Complaint Handling

a) Inclusion of the Postmaster Experience Forum which is the forum that collates postmaster complaint causes with other postmaster insights and reviews them in a cross functional meeting, which includes postmaster representation.
b) Addition of the service levels Post Office aim to address complaints within.
c) Clarity around how Executive complaints are dealt with.
d) Removal of a section referring to the Investigations Policy as this is being rewritten.
e) Amendment to the process for the closure of a complaint, putting focus on a postmaster's option to dispute.

Related Postmaster Complaint Handling policy assurance actions

Six actions were identified by Group Assurance.

Of these, three are closed:

- Reintroduce the Voice of the Postmaster Forum (which was done by introducing the Postmaster Experience Forum)
- Reintroduce meetings between the Issue Resolution and Speak Up Managers (this is now used to Quality Assure decisions relating to Speak Up characteristics)
- Introduce tracking of service level data

The other three are complete and evidenced by the policy, which is being reviewed by Group Assurance:

- Redraft risks
- Redraft Controls
- Introduce the Service Levels into the policy

13

Network Monitoring and Branch Assurance Support

a) Significant change to a branch visit. Previously, a contract advisor would be contacted for any discrepancies found over £2000 (Local model/SPSO) or over £5000 (Main model). Following approval at Retail Committee on 9th April, a contract advisor will now only be contacted if there is an admittance of theft or misuse of Post Office funds.

b) Minor wording changes and additional sentences to support new ways of working:
   - Made it clear that currently visits will not take place if the postmaster hasn't been informed and removed reference to "unannounced visits".
   - Removal of Post Office contractual rights regarding losses, as this is not relevant to the role of Branch Assurance.
   - Clarity around what happens when a discrepancy is found, and the support signposted to the postmaster (Branch Support Centre and NFSP)
   - Mention of the new Quality Assurance process by Assurance and Complex Investigations.
   - Mention of the new Postmaster Feedback method.
   - Mention of the weekly stakeholder meeting.

c) Removal of a control to ensure known errors are checked before each visit, as this is no longer relevant to the branch assurance role, which is simply to count the cash and stock.

d) Removal of non-suspension monitoring section.

Related Network Monitoring and Branch Assurance Support policy assurance actions

Five actions were identified by Group Assurance.

One is closed:

- Branch Assurance Quality Assurance relaunch

Two are complete and evidenced by the policy, which is being reviewed by Group Assurance:

- Redraft risks
- Redraft Controls

It has been agreed with Group Assurance that the final two actions are not able to be evidenced directly by the policy but relate to discrete pieces of work:

- Introduce end-to-end view of the network through MI (a revised dashboard to replace the Retail Performance Dashboard is currently being created)
- Introduce clear KPIs to capture both quantitative and qualitative impact of activities undertaken (a 1st line Policy Assurance framework and schedule is planned to be implemented, by the end of Q2)

13

Network Cash and Stock Management

a) Addition of a specific Foreign Currency discrepancy procedure for clarity.

b) Amendments relating to stock ordering being managed by the Inventory Support Centre instead of the Branch Support Centre.

c) Addition of a paragraph on expectations around excess stock (anything over 12 weeks).

d) Removal of dispute escalation to the Decision Review Panel. The reason for this is that in three years no discrepancy has required escalation. The panel now only hears

Contract Termination challenges, but as Post Office develops a loss recovery process, a new forum will need to be created to hear escalated discrepancy cases.

e) New section on external assurance (ISO9001 and PwC)

Related Network Cash and Stock Management policy assurance actions

Two actions, both relating to policy controls, were identified by Group Assurance. They are both complete and evidenced by the policy, which is being reviewed by Group Assurance:

- Redraft Controls
- Implement control standards for the return of excess cash

How are the policies working in practice?

5. In March, ARC suggested that it would be useful, in future policy papers, to briefly describe how we know the policies are working and what our colleagues think about the application of the policy.

6. The Retail Performance Dashboard tracks metrics relating to each of the policy areas and allows the Retail Committee and SEG on a monthly basis, and Board on a quarterly basis, to identify any areas of concern. Specific to these policies it shows the number of complaints received from postmasters, and the main reasons for those complaints, the number of discrepancies found in cash pouches and the volume of activity carried out by the Network Monitoring and Branch Assurance teams.

Group Assurance have provided feedback on how the dashboard can be improved to provide more evidence of how the policies are working in practice, and this is in progress.

7. Seeking feedback from postmasters for each policy area is important to us, and for these policies we know that:

a) 93% of postmasters (for FY 23/24), agreed or strongly agreed that they were satisfied with the knowledge and expertise of the advisor they spoke to in the cash management contact centre.

b) 1849 (for FY 23/24) postmaster complaints were dealt with by the Issue Resolution team, and escalation requests were received for only 3% of cases. Complaints are included in postmaster insights that are discussed and addressed at the Postmaster Experience Forum.

Postmaster feedback is an area we are going to be working more on in the next few months – for example, the Branch Assurance team have created a letter to leave with postmasters following a Branch Assurance visit to request feedback, via a QR code.

13

8. For these policies we've reached out to a selection of colleagues and 100% of them are aware of the policies and know where to find them. We've received some positive comments on how important the policy is to colleagues' roles, how the policies are up to date and give clear guidance, the usefulness of the procedures, information and reporting links and how they ensure that colleagues follow the principles.

9. The National Federation of Sub-Postmasters have been consulted and are satisfied with the changes made to these policies.

10. Please see Appendices 1 to 7 showing marked up versions of each policy, clean updated versions and a more detailed summary of all changes made.

Next Steps & Timelines

11. Work will continue on the completion of the two outstanding actions.

12. Following approval of the policies, Post Office will ensure that:

- All relevant teams and stakeholders are fully trained on the updates to the policies by the end of June 2024.
- The updated policies will be made available on the Post Office Intranet site.

13. The following policies are planned for June RCC and July ARC:

- Postmaster Account Support
- Postmaster Accounting Dispute Resolution

13

Appendices

All appendices are available in the Diligent Reading Room

1. Postmaster Complaint Handling Policy V3.0 Marked up
2. Postmaster Complaint Handling Policy V3.3 PDF
3. Network Monitoring and Branch Assurance Support Policy V3.0 Marked up
4. Network Monitoring and Branch Assurance Support Policy V3.3 PDF
5. Network Cash and Stock Management Policy V3.0 Marked up
6. Network Cash and Stock Management Policy V3.2 PDF
7. Postmaster Policy Review Changes

13

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	21st May 2023
Author:	Reena Chohan, Policy Compliance Manager	**Sponsor:**	Jonathan Hill Group Compliance Director / Ben Foat, Group General Counsel

Input Sought: Approval

The Committee is asked to review and approve the following updated policy for the business to take forward:

i. Cyber and Information Security Policy;
ii. Business Continuity Management Policy;
iii. Speak Up Policy and
iv. Employee Vetting Requirements Policy

Previous Governance Oversight

Risk & Compliance Committee (RCC) 7th May 2024

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 ARC to consider.

Questions addressed

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
Cyber and Information Security Policy	March 2023	**Minor** updates this annual review	Group Chief Information Officer	RCC/ARC
Business Continuity Management Policy	May 2023	**Minor** updates this annual review	Interim Group Chief Finance Officer	RCC/ARC
Speak Up Policy	May 2023	**Minor** updates this annual review	Group General Counsel	RCC/ARC
Employee Vetting Requirements Policy	January 2023	**Minor** updates this annual review	Group Chief People Officer	RCC/ARC

What updates were included and why?

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

2. Cyber and Information Security Policy: The policy has had **Minor** changes and the following updates were made to the policy this annual review:

a. Minor updates to reflect changes in organisation structure, align with Policy Document template.
b. The core principles section has been enhanced to provide additional clarity.

The policy owner has confirmed in their attestation, the quarterly control attestation process confirms that a number of controls are not currently being met, further work is also required to confirm the coverage and effectiveness of those controls that are stated as met through the attestation process. As part of the quarterly IT Control submission this provides an overview of the compliance status to the Cyber and Information Security Policy controls. This is further supported from the alerts we receive from the SOC team and a number of approved Policy Exception Notes are also in place, these are managed through the standard PEN process.

3. Business Continuity Management Policy: The policy has had **Minor** changes and the following updates were made to the policy this annual review:

a. Reviewed the risk tolerance statements to ensure still accurate.

The policy owner has confirmed in their attestation, that the required operational standards stated within the policy are working, being met and can be evidenced. A biennial BIA programme is completed with Business Continuity Plans created. BC training is completed with a set group of colleagues to manage incidents effectively and tests are conducted throughout the group. Building resilience reviews are ongoing to ensure they meet our recovery strategies.

4. Speak Up Policy: The policy has had **Minor** changes and the following updates were made to the policy this annual review:

a. Minor appointment name changes from CIU to A&CI, Head of CIU to Director of Assurance &Complex Investigations

The policy owner has confirmed in their attestation that the required operational standards stated within the policy are working, being met and can be evidenced. The Control measures form the continuous Comms Plan which is implemented by the SU Team and those who also have obligations to promote SU.

14

5. Employee Vetting Requirements Policy: The policy has had **Minor** changes and the following updates were made to the policy this annual review:

a. 1.4 Application – first paragraph where is says (Post Office Insurnace and PayZone), Insurance was previously spelt wrong, but we need to put 'Post Office Insurance, Postmaster/Agents and will apply to Payzone from 1st May 2024.
b. 2.2 Policy Framework
c. 2.4 Control Measures - Added
d. 5.1 Document Control Record:
GE Policy Sponsor – Group Chief People Officer , Karen McEwan
Standard owner – People Director – Services – Tim Perkins
Standard Implementer – Head of People Support Services
Standard Approver – Head of People Support Services.
Revision History– needs adding to; 6, 28/02/2024, Martin McKee
e. 5.3 Company Details – registered address needs updating to Wood Street
f. Appendix A – New POL Employee, need to add '(up to and including SLP) before EXCLUDING
g. Appendix A – CEO and GE – remove SLP, need to amend 10 year work history to say 5 year work history (unless CViT)

The policy owner has confirmed in their attestation, that the required operational standards stated within the policy is being met and can be evidenced.

6. The policies in both clean and tracked changed versions can be found in the reading room.

7. Assurance

Group Compliance have commenced Policy Compliance Reviews and are in the process of testing and assuring the Procurement Policy and Health & Safety Policy. The outcome of the reviews and the report will be shared with the RCC and ARC in due course.

The purpose of the Policy Compliance Review is to understand, test and gain assurance based on some point of control testing that the Group Key Policies that Post Office Limited have in place are: -

- working in pursuit of day to day business;
- the policies are being effectively implemented across the group and that compliance with them is being met;
- the policies have effective required operational standards to mitigate any risks that may arise.

7. 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.

14

Policy Appendices

1. Cyber and Information Security Policy (Clean)
2. Cyber and Information Security Policy (Track Changed)
3. Business Continuity Management Policy (Clean)
4. Business Continuity Management Policy (Track Changed)
5. Speak Up Policy (Clean)
6. Speak Up Policy (Track Changed)
7. Employee Vetting Requirements Policy (Clean)
8. Employee Vetting Requirements Policy (Previous Version)

14

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Post Office Insurance ARC Update	**Meeting Date:**	21 May 2024
Author:	Ian Holloway, Director of Risk and Compliance	**Sponsor:**	Clare Ryder, POI NED and POI ARC Chair

Input Sought: For Noting

Previous Governance Oversight

This paper is a regular update paper for the Committee. It provides key information on our significant risks, how these risks are being controlled and any gaps in control.

Executive Summary

The full year 23/24 trading performance for POI remained strong with an EBITDA trading performance of IRRELEVANT Some periodic impact to current performance is being experienced as a result of the Horizon IT Enquiry and the related ITV Docudrama. This has impacted both customer propensity to purchase our products and also at times has limited our ability to carry social media and TV adverts. A watching brief is being maintained as the enquiry progresses though there is no indication at this stage that any brand damage is permanent. We have raised the score of our reputation risk to a residual of 12 which we feel fairly reflects the potential impact on POI.

Cyber remains the highest graded risk within the POI business. Good progress has been made in strengthening POI specific controls and further review by Deloitte has commenced. POI note our dependency on the wider POL cyber environment and the Group cyber improvement plan to further reduce the potential impact of our exposure. We understand that exact budget and timescales are still being agreed.

POI has now successfully delivered the transition of our household call-centre from First Source to Webhelp after a challenging start to the project. Initial performance indications are positive though Management remain vigilant in this early period post transition.

The FCA wrote to POI on 17 April 2024 with a further information request on how POI oversees POL as an Appointed Representative (AR). The request focuses on how conflicts of interest are managed, our capital position and our key oversight controls. POI has responded in full and no FCA response has yet been received. AR oversight controls remain a key focus area for the FCA and given the current publicity surrounding POL it should be expected that the FCA may return with further questions. A separate paper presented at this meeting covers the importance of oversight controls.

The FCA has also written to POI specifically to remind us of our obligations to review our due diligence on key POI and POL staff in the light of any findings produced by the Horizon IT enquiry. POI has in response noted that it has appropriate due diligence processes and will continue to review all relevant matters.

By mutual agreement the POI Chair Tim Franklin will be leaving POI on 30 May 2024. This follows completion of a second term of office. A search for a replacement is currently underway.

POI have raised a specific risk relating to Executive and Senior Management recruitment. Feedback from our Executive recruitment partner suggests that the Horizon IT Enquiry is impacting the willingness of senior staff to apply for Post Office related jobs and that the current pay on offer for NED roles is significantly below the average for financial service roles of a similar type. Discussions are ongoing to find a solution to these issues.

IRRELEVANT

April mystery shopping results show an overall pass rate of 64% for travel and 83% for protection sales within the branch environment. The travel score is down from an average of c80% in recent months. The key failure point for travel is again a failure to provide customers with the leaflet which contains the levels of cover, policy exclusions and limitations. Further analysis shows that over the period there were supply problems with the leaflet which has undergone some minor changes. For protection the main failure causes were failing to provide the policy summary and failure to clearly ask the smoking question. We are working with retail Management to address these issues.

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	IR35 - Engagement of contractors – risks and decisions	**Meeting Date:**	21 May 2024
Author:	Tom Lee, Group Financial Controller Andy Jamieson, Head of Tax Tim Perkins, People Services Director Racheal Hill, Head of Talent Acquisition	**Sponsor:**	Kathryn Sherratt, Interim Chief Financial Officer Karen McEwan, Chief People Officer

Input Sought: Noting and comment

The ARC is asked to note the status of the financial risk stemming from the tax treatment of contractors under IR35, including a timeline of events and advice taken, alongside the businesses proposals regarding the contractor population and reducing any future financial tax risk connected to IR35.

Previous Governance Oversight

- ARC paper of 12 March 2024 – "IR35 - Engagement of contractors – risks and decisions"
- ARC paper of 23 January 2023 – "Tax Update and Annual Tax Strategy"
- ARC paper of 24 Jan 2022 - "Tax Update"
- ARC paper of 17 May 2022 – "Tax Update – IR35"
- ARC paper of 29 March 2022 – "Future Contractor Profile"
- ARC paper of 24 January 2022 – "Tax Update"
- ARC paper of 30 November 2021 – "Tax Update
- ARC paper of 12 January 2021 – "Tax Update"
- ARC paper of 28 January 2020 – "Tax Update"

Executive Summary

In March 2024 a paper regarding the contractor population and the associated IR35 risk was presented to RCC and ARC. This paper addresses the ARC actions following the March meeting which included a) to provide a history regarding the IR35 risk and b) advise on what actions the business proposes to take in relation to the contractor population and the associated IR35 risk.

Regarding the history, both a detailed timeline (Appendix 1) and a key points section has been presented. This shows that the HMRC review has been ongoing since 2018 with the depth of questioning increasing in recent years and HMRC not presenting their view until December 2023. In late 2016 POL engaged external tax advisors to assist and advise on the implementation of the revised IR35 legislation which took effect from 1 April 2017. After the legislation became effective external expertise has been provided to POL to assist in understanding the developments in IR35 and in complying with HMRC's revised guidelines, reviewing our policies and, from early 2019, the HMRC review itself, with Deloitte initially involved and KPMG taking over from September 2022. POL also employed a highly experienced employment tax specialist in 2021 to assist in this area. ARC have been kept abreast of the situation since 2020, with the only notable decision being made in 2022 when GE were tasked with addressing the future risk arising from IR35. A plan was put in place to bring all contractors inside IR35 from September 2022, however following government u-turns on policy decisions in this area during September and October of 2022 the planned changes were cancelled. ARC were advised of this position in January 2023 with no further action required. POL are currently debating HMRC's view on POL's right to reject a substitute, which is a key clause impacting the determination of Inside vs Outside IR35.

To help mitigate future liabilities in this area a Contractor Review Project has been implemented and SteerCo and Working Group established, with several key workstreams - the review of Outside IR35 contractors being the priority. With the support of SEG, the first stage of the project is to conduct an impact analysis assessing criticality of role, contingency plan and duration of activity required amongst other items. This activity is due to be completed by 10th May which will enable full completion of the programme plan.

RCC are requested to review and comment on this paper prior to onward submission to ARC.

Questions addressed:

1. What is the history of the IR35 risk and business actions?
2. What is the status of the HMRC review and the next steps?
3. What are we going to do to mitigate the risks regarding the current and future contractor population?

Report

Historical assessment of the IR35 position

1. A detailed history is included in Appendix 1 of this paper, with the below summarising the key points for the committee to note.

2. The revised IR35 legislation was introduced in April 2017. From late 2016 POL began to prepare for its introduction, with the Cost Reduction Group being made aware of the requirements and likely impact. In 2017 training was also provided to the Talent Acquisition ("TA") team by Deloitte on how to run CEST assessments, with test CESTs run with Sopra Steria, the original Managed Services Provider ("MSP"), to confirm answers were being interpreted correctly.

3. HMRC first contacted POL regarding their intention to check compliance with the legislation in 2018, with initial correspondence between HMRC and POL being slow and limited in terms of the nature of questioning. This remained the case until July 2019 when the level of information requested by HMRC deepened. POL continued to respond to HMRC's queries, which were delayed in 2020, due to Covid 19. Until this point POL had relied on external support to advise on any employment tax issues. However, in March 2021 POL recruited an employment tax specialist to provide further strength to the team, with the individual having 20 years' experience at HMRC followed by a career in practice, including big-4 firms.

4. The depth of questioning from HMRC increased notably in 2022, albeit the speed of their communications remained slow. This uptick followed POL providing evidence of a

substitute being used by a contractor, culminating in 83 questions being asked in May 2022. It was expected that the responses to these would be sufficient for HMRC to provide a view, however some further queries were raised in November 2022 and it wasn't until December 2023 when HMRC presented their stance, albeit in a manner that was ambiguous as to how they formed their opinion.

5. Throughout this period POL management have kept ARC up to date with the status of the HMRC review and the actions being taken, with regular updates provided from 2020 onwards. In November 2021 ARC were advised that the "substitution clause" was a key driver in the determination of the inside vs outside IR35 assessments, that only 1 example had been identified within POL and that if HMRC disagreed with the treatment there was significant financial exposure, subsequently estimated in May 2022 to be £70m-£80m + penalties in a worst case position. Updates thereafter built on these points.

6. Following the May 2022 IR35 update to ARC, and building on a paper presented by the People team in March 2022 regarding the future contractor population and the plans to reduce this, ARC agreed that action should be taken to mitigate the future financial tax risk, whilst noting that any wholesale changes could present a risk with regards to the HMRC review and how they may perceive it, with the GE taking an action to address the future risk.

7. In June 2022 GE established a Steerco on this matter, with the decision taken to change the policy on substitution which would be likely to have the effect of bringing the majority of contractors inside IR35. This was due to be enacted in September 2022 (over a 6 month period whilst contracts were renewed) however the day before the announcement was due to be shared across the business Kwasi Kwarteng announced the repeal of IR35 legislation with effect from 1 April 2023. As a result the Steerco determined that the changes should be abandoned given the future risk would be eradicated in several months time. Jeremy Hunt then reversed the policy decision in October 2022 and there was talk of an IR35 consultation being launched, which subsequently led to tax offsets being announced. The government flip-flop and announcements indicated indecision at a policy level and therefore uncertainty on the future of IR35 legislation. Given POL's planned changes would have resulted in increased immediate costs from bringing individuals inside IR35, potential loss of resource which could have jeopardised the delivery of business critical projects and the planned migration to a new MSP, Morsons, the Steerco determined to abandon the changes and disband the Steerco.

8. The events and decisions presented above were brought to ARC in Jan 2023 with no further action requested i.e. ARC were content to await HMRC's decision. In hindsight, had the business known HMRC would not state their view until December 2023 and alternative approach may have been taken.

9. POL and HMRC are currently engaging around the decision making that has led HMRC to their views, as the correspondence to date isn't compelling in POL's view. POL have a draft letter awaiting to be sent to HMRC to challenge their views further, albeit noting the likely outcome being HMRC will not change their stance based on historical dealings with them.

10. Throughout this process POL management have engaged with specialists:

    a. Deloitte were engaged from 2016 through to 2022, initially to assist with the implementation of the IR35 policy, including training POL management and assessing interpretations for the CEST Tool. Deloitte support then expanded into reviewing the HMRC requests and advising on POL correspondence given their knowledge of the subject and POL's policies.
    b. POL employed an Employment Tax specialist in March 2021 to review the position, correspond with HMRC and assist the People team in this area. The individual has in depth knowledge on this subject, including creating an IR35 assessment tool used in practice.
    c. [redacted]
    d. Given the shift in HMRC focus a tender exercise was run, with KPMG tax and legal being appointed from September 2022. All correspondence has been reviewed and advised on by KPMG in this period. At no point have Deloitte or KPMG advised that POL's approach has been incorrect, but there was recognition when KPMG came on board that any reassessment by HMRC across some roles may present a risk.

11. The risk and status has been known by UKGI and DBT, through UKGI representation on ARC and Board throughout the period, in addition to regular discussions on this topic for the purposes of the Annual Report and Accounts in regards to disclosure and funding requirements.

Current status of the HMRC review

12. [redacted]

13. Subsequent to the above, POL have been in communication with HMRC to seek clarity on their rationale. POL have a further response prepared, see above, which is to be reviewed by KPMG before issuing, in line with previous communications on this matter. However, [redacted] the letter has not yet been issued.

    In addition, HMRC have recently issued 'protective assessments' dating back to the tax year 2017/18, to ensure that they are not out of time for raising an assessment, if they conclude Post Office has been incorrect in its approach. The assessments cover PAYE, NICs and Apprenticeship Levy, all of which would have been due if contractors should have been Inside IR35. POL has appealed against the assessments as HMRC have not issued a decision as yet. They confirmed recently in a call that there was 'no decision' as yet. HMRC can go back 6 years if they consider Post Office has not taken 'reasonable care' in managing the tax position.

Next steps with HMRC

14. As stated above, the next step with HMRC is to reply to their letter of 21 March where they set out further clarification of their view and also their view on the next steps. We will respond once POL legal and KPMG have reviewed and advised.

15. HMRC's view is that POL has a contractual right to reject a substitute (set out in 19 December 2023 letter). However, in the 14 February 2024 email they suggest that one example of a substitute, which was supplied in detail in December '21, is not sufficient – they also question whether would POL accept substitutes in all roles – indicating that they might accept that POL can accept substitutes in some roles.

16. HMRC refuse to provide examples of contracts they have seen between an Agency and Contractors stating that they cannot do so under GDPR. However, they infer that there is something in these contracts that indicates we have a contractual right to reject a substitute. We have asked HMRC to confirm what it is they draw from the contracts if they cannot provide them, they state they are unable to do so.

17. HMRC state that POL's Policy on engaging contractors suggests it has the right to reject as it states POL can do so if the substitute contractor is not suitably qualified and does not pass any security clearance required. These are standard terms and conditions that any business would apply and should not constitute a right to reject.

18. Regarding HMRC's next steps they suggested that POL supplies names and contact details of all contractors so that they can contact a sample, and also contacts at Morson and Intelligent Resource. As there are over 1,500 contractors POL has used since April 2017 this is not practical.

19. POL's suggestion, which was agreed by KPMG, was so seek HMRC's approval for POL to sample check contractors in different roles across the years, to re-assess the outcomes. This would then be reviewed by an external third party.

20. POL will also seek to understand how the tax offset announced by HMRC to take effect from April 2024 will work in practice and then look to [redacted] HMRC based on the above.

21. Since Morson took over as POL's MSP, in January 2023, there has been a decrease in the number of contractors for IR35 consideration. Around 40% of contractor now are supplied through umbrella companies, meaning that they pay PAYE and NICs and there is no risk arising of tax owing for POL. However, the remaining balance still are largely Outside IR35. This will be examined in detail by TA with Tax team support, as Morson's processes do not allow for a substitute. This should mean that a larger proportion are more likely to be Inside IR35. At present this does not appear to be the case.

What are we going to do to mitigate the risk of the current and future contractor population?

22. To mitigate the risks of current and future IR35 related liabilities a Contractor Review Project has been initiated with Executive sponsorship of the Chief People Officer. The project's working group includes a range of subject matter experts from across the business and a full time Project Manager has been assigned to the project.

23. The initial workstreams that have been identified for the project are:

    a. Reviewing active Outside IR35 contractors;
    b. Reviewing contractors with over 2 years tenure;
    c. Reviewing all other active contractors;
    d. Reviewing all contractor related policies, processes, and governance; and
    e. Working alongside the separate procurement exercise being carried out to resolve governance and procurement issues identified with the existing contingent labour contract.

24. The table below shows the contractor population working in POL as of 26th April 2024:

Function	Active Contractors	Outside IR35	Over 2 Year's Tenure	"Highly Skilled"
CEO Office	1	0	0	0
Commercial	26	11	13	1
Finance	5	2	2	0
Inquiry	19	4	4	3
Legal	1	0	0	0
People	11	11	1	8
Remediation Unit	85	46	24	11
Retail	18	8	5	2
Strategy & Transformation	7	3	4	0
Technology	169	88	63	24
Total	342	173	116	49

25. The Strategic Executive Group (SEG) and the Finance Directors have now conducted an impact analysis on this population. The impact analysis assessed:

    a. the criticality of active contractors (critical, important, semi-important and not important)
    b. the rationale for this rating
    c. anticipated end date of activity; and
    d. whether the contractor is truly a highly skilled (this is considered one of the determining factors of an Outside IR35 result).

    A decision tree was created to support these assessments.

26. The outcome of the initial criticality assessment is as follows:

	Critical	Important	Semi-Important	Not Important	No Longer Required	Review Outstanding	**Total**
CEO Office	1						1
Commercial	16	5	2			3	26
Finance	2		3				5
Inquiry	14	5					19
Legal		1					1

People			3	8			11
RU	20	51		14			85
Retail	8	7	1		2		18
S&T	2	3	2				7
Technology	64	77	28				169
Total	126	149	39	22	2	3	342

There remain 3 contractors to review in Commercial that have not been able to be reviewed yet due to absence of the key business stakeholder for those contractors.

Whilst the initial criticality assessment has been completed, further review is required of the responses to ensure consistency across the business.

27.The assessment of whether the contractor is truly highly skilled has resulted in 33 of the contractors originally deemed highly skilled to not be assessed as being highly skilled. The remaining 16 contractors who have been assessed as being highly skilled will be reviewed by the Tax team to provide assurance of their highly skilled status.

28. Once these further reviews are complete, the following will be assessed or created:

a. The feasibility of mitigating current and future IR35 related liabilities;
b. A timeline detailing what actions can be taken when to mitigate current and future IR35 related liabilities whilst minimising delivery disruption;
c. The level of retained IR35 risk once all actions have been taken; and
d. Policies, processes, and governance that ensure that POL maintains or continues to reduce the retained level of IR35 risk on an ongoing basis.

Timelines are not finalised or agreed on these deliverables for the project yet, but indicatively (a) will be complete by the end of May, (b) and (c) will be completed in June and updates on (d) will be provided to the July ARC.

29. Depending on the level of change required in the contractor population, the project may also, in addition to the deliverables above, need to oversee the ongoing mitigation activities outlined in the timeline.

30. It is worth noting that POL has changed its approach to engaging new contractors since moving the contract for contingent labour to Morson (as the managed service provider (MSP)) from January 2023, which has in turn reduced the existing IR35 risk. As set out in the 12th March paper, the new contractor population has a lower number of Outside IR35 determinations than under the previous MSP. This is largely due to c50% of new contractors being engaged through umbrella companies, rather than through the IR35 assessment process. Of the remaining new contractors (those engaged outside umbrella companies), >90% of engagements remain Outside IR35, which is still very high and contrary to hiring in the general contractor sector outside of POL. In terms of existing (and therefore longer serving) contractors, 32% of active Morson contractors transferred over from Intelligent Resource (the previous provider of contingent labour to POL), of which, 75% are engaged Outside IR35.

31. As referenced above, there are also a number of procurement and governance issues that need to be resolved with regards to the contingent labour contract. The Contractor Review Project will oversee resolution of these issues. The issues are:

    a. POL has exceeded the total contract value for the contract awarded to Morson. A modification to the existing contract and a re-procurement are therefore required (and will go through SEG and Board).
    b. The contract award notice for Morson was never published. SEG have agreed to publish this immediately.
    c. POL continue to have a payroll contract with Intelligent Resource which ends in March 2025. 18% of POL's active contractor base are still engaged via Intelligent Resource and will need to move to Morson or another contingent labour provider from March 2025 at the latest.

Appendix 1 – detailed history of the IR35 position

2016

1. POL - the Cost Reduction Group were advised of the expected changes and impacts of HMRC's planned IR35 legislation.

2017

2. POL - the Talent Acquisition ("TA") team received training from Deloitte and ran test CESTs with Sopra Steria, the original Managed Services Provider ("MSP"), and received confirmation they were interpreting the answers correctly. The TA team continued to run the CEST review process thereafter.

2018

3. HMRC - in June 2018 HMRC wrote to POL to 'check compliance' and asked for a description of how POL had complied with the IR35 legislation. Following some initial delays in responding, exchanges of information occurred with HMRC through to July 2019.

2019

4. HMRC – planned to introduce new legislation for IR35, impacting the private sector, from April 2020.

5. POL - in December 2019 POL Tax sought further advice and training from Deloitte to assist HR colleagues on using the new CEST tool. A training session was run for the POL TA Manager and team.

2020

6. POL - sought training from HMRC in Jan 2020 on the use of a new CEST, following the planned introduction of new rules for IR35 from April 2020. HMRC cancelled the training and the introduction of the new rules was subsequently delayed until April 2021 due to Covid 19.

7. ARC – at the January 2020 ARC an update was presented on IR35 noting that HMRC have an ongoing review which could result in financial impacts, internal assessment shows the CEST tool may have been incorrectly applied in some instances and Deloitte were supporting in an assessment of the position.

8. HMRC – in October they followed up on responses provided by POL to previous queries, from July 2019.

9. POL – determined it was appropriate to recruit an employment tax specialist to help address the queries. Agreed with HMRC that responses would be delayed until in house expert recruited.

2021

10. ARC – at the January 2021 ARC an update was presented on IR35, including details of planned recruitment of an Employment Taxes specialist, HMRC review ongoing and level

of queries increasing, responses being prepared for HMRC and noting that it appeared HMRC's tests had been applied in a consistent manner in line with guidance.

11. POL - in March 2021 the post was filled by ex-HMRC Inspector with 20 years Employment Tax Advisory experience, an IR35 expert who had developed Grant Thornton's IR35 software tool, started in post at POL. He assessed POL's position, revisiting earlier evaluations and concluded that although certain CEST questions may have been incorrectly answered, the outcome of Outside IR35 remained correct on the basis that POL had no right to reject a substitute if one was required/ provided. Noting this latter point is crucial in the assessment.

12. HMRC - in May 2021 responses were provided by POL to queries received from a new HMRC officer. Further back and forth on queries occurred between September and December.

13. ARC – at the November 2021 ARC a specific paper was presented on IR35 compliance. [redacted]

2022

14. HMRC - In Jan 2022 HMRC asked for more evidence around the example of a substitute in POL's business, this was supplied providing contracts, copy invoices, etc, in the same month. HMRC continued to state they were 'fact finding' and provided no indication that they believed POL's approach was incorrect.

15. ARC – in Jan 22 a general IR35 update was provided as part of a wider Tax update. Noted Deloitte, [redacted] and People teams were assisting with the HMRC responses and that POL faced significant financial risk if HMRC have found incorrect application. Additionally, one instance of a substitute had been identified, with documentation provided to HMRC following Deloitte review. Identifying substitutes was difficult as the process in place would not require the use of a substitute to be recorded by the business or the TA team.

16. ARC – at the March 2022 ARC a paper was present by the People team on the Future of Contractors within the POL business. This focussed on the need to reduce reliance on contractors. The increased use had been driven by the requirement to reduce headcount, however, large business critical projects such as SPM and RU activity put pressure on the business to use contractors. It was stated that plans were in place to convert contractors to FTC and permanent roles.

17. HMRC - in April 2022 HMRC introduced an IR35 specialist team (and the 4th different officer looking at the case), promising to bring the matter to a conclusion. In May 2022 HMRC wrote an 11 page letter asking 83 questions around the contract between POL and

Sopra Steria. POL decided at this point that many questions were contract law questions and not tax questions and went to tender for support in answering, KPMG Legal and Tax were appointed and helped the Tax team send a 21 page response to HMRC's questions, in September 2022. Based on discussions with HMRC it was expected that they had all the information required to make a decision.

18. ARC – at the May 2022 ARC the Tax team confirmed there remained concern over IR35, the historical risk was £80m plus penalties, there was large reliance on the substitution clause of which we only have 1 example and that it was clear HMRC will continue to look in depth at the position. [redacted]

19. GE - in June 2022 a paper was presented to GE recommending that the Policy was changed to de-risk the tax position, with Outside IR35 being an exceptional treatment rather than the norm. A SteerCo involving CIO, CFO, CPO and Tax and TA was set up to oversee the project reviewing the position and making recommendations. The paper recommended that for all new engagements and renewals of contractors that they be engaged on an Inside IR35 basis. GE approved the project, though concerns were expressed over the potential commercial implications if bringing contractors Inside IR35 resulted in an increased cost base.

20. Steerco - in August 2022 plans were confirmed including revised policy and draft comms, to advise contractors of the move to bring individuals inside IR35, over a 6 month period. Comms were planned for 23 September 2022 however in an unexpected move Kwasi Kwarteng announced as part of a mini-budget the repeal of IR35 legislation with effect from 1 April 2023. The SteerCo was approached and a unanimous decision was made to cancel the project and to maintain the process based on no right to reject a substitute.

21. Steerco - On 17 October 2022 Jeremey Hunt, the new Chancellor, announced a u-turn, scrapping Mr Kwarteng's repeal of IR35 and continuation of the existing rules. In mid-November 2022 the SteerCo held a call regarding the u-turn. It was concluded that in light of the reversion to the post April 2017 rules that the business awaited HMRC's decision. The increased immediate cost of bringing individuals inside IR35, the potential loss of resource, the tender to appoint a new MSP, and therefore jeopardising the delivering of business critical projects swayed the decision. With hindsight had we known HMRC would take a further 14 months to issue an opinion, which is still not a firm decision, the business decision may have differed. Any change in Policy enacted in November 2022 would have only prevented a tax exposure from that date and not altered the historic position. The new MSP, Morson, has provided greater challenge to status determinations and around 40% are now provided through Umbrella companies, removing POL's tax risk on this proportion.

22. HMRC – in November 2022 HMRC asked further questions, most of which have already been answered in earlier communications. POL provided an 11 page response to HMRC's questions in December 2022.

2023

23. ARC - in January 2023 the Annual Tax Update was presented to ARC including a section on IR35. The SteerCo decision was explained, as stated above, with ARC accepting the position taken. HMRC continue to ask further fact-finding questions.

24. HMRC - on 6 April 2023 HMRC sent a 5 page letter containing 30 additional questions. POL provided a 12 page response to HMRC on 19 June following KPMG Tax & Legal review. Further correspondence was received from HMRC in August and October advising of absences in their team causing delays but that they expect to respond by the end of October. On 19 December 2023 HMRC responded with their 'opinion' that POL have a contractual right to reject a substitute.

2024

25. POL - HMRC's letter of 19 December was not entirely clear. POL discussed it with KPMG and then held a call with HMRC to seek clarity. On 7 February 2024 POL requested confirmation in writing of some of the points HMRC raised in the call. HMRC responded by email on 14 February setting out that one example of a substitute is, in effect, not enough to convince them, stating that consideration needs to be given as to whether POL would accept a substitute in each and every role. Further correspondence between POL and HMRC was held, to seek clarity on HMRCs view with POL now due to respond to HMRC, albeit the response is on pause [redacted]

26. ARC - on 12 March TA and Tax team present to ARC setting out the financial risk that is beginning to crystallise now that HMRC have provided their opinion and some clarity on their thinking.

27. HMRC - on 2 April HMRC raised a protective assessments totalling £27m. These cover 2017/18 to 2019/20. The assessments are raised to prevent earlier years falling out of time for HMRC to assess, should they conclude that POL has been wrong since April 2017 in its categorisation. HMRC make clear in a call that the assessments are not an indicator of a decision, the matter is still under consideration and they are issued on a worst-case basis as HMRC cannot increase an assessment once 6 years has elapsed, but can reduce one. POL appeals against all the assessments.

17

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Tax Update and Annual Tax Strategy	**Meeting Date:**	21 May 2024
Author:	Tom Lee, Group Financial Controller Andy Jamieson, Head of Tax	**Sponsor:**	Kathryn Sherratt, Interim Chief Financial Officer

Input Sought: Noting and Approval

The Audit, Risk and Compliance Committee ("ARC") is asked to note the Tax Update and approve the Tax Strategy following the annual review.

Previous Governance:

Approved by Risk and Compliance Committee on 7 May 2024.

Executive Summary

This paper is an annual tax update, the last of which was presented to the ARC in January 2023. The paper provides an update on tax for the ARC to note and discuss, as well as providing a copy of the tax strategy following for its annual review, last published in January 2023 (the "Tax Strategy"), for the RCC to approve ahead of submission to ARC for final approval. No significant updates have been made to the Tax Strategy compared with the prior year.

Questions addressed

1. What are the strategic tax challenges for POL?
2. What are the current key tax issues for POL and what are we doing to address these?
3. What other tax updates should the RCC be aware of?
4. What is the requirement for reviewing and updating the published tax strategy?

Report

What are the strategic tax challenges for POL?

1. The current primary tax risks are around our management of employment taxes and a specific potential corporation tax (CT) issue, linked to expenditure incurred, settlements made and funding receipts received from DBT for the OCC, HSS, PPR, SRR and Tax top ups – 'the schemes'. VAT compliance remains a risk due to the throughput of tax and the complexity, but with much improved processes and controls the risk and incidence of errors has reduced.

2. Our relationship with HMRC has become more challenging over the past couple of years. This appears to be driven by a number of factors including i) the complexity of items we are engaging with them on, which have become more challenging recently (CT and ET in particular) ii) the speed of their response, they are extremely slow to respond in general, with responses taking c. 4-6 months and iii) they do not appear prepared to approach issues with commerciality or pragmatism in mind. Based on conversations with tax advisors and other business contacts this shift has been consistently noticed across the tax paying community. This shift is making it difficult to manage our taxation position effectively, with risk and exposure continuing to increase.

Current Key Tax Issues

Employment Tax, IR35 – correct treatment of contractors' employment status

3. A full paper covering this topic is being presented at RCC separately. We have therefore not commented in any detail in this paper. HMRC have reached an opinion that we have a fettered (contractual) right to reject a substitute which, if correct, would mean that we have completed the check employment status for tax (CEST) (HMRC's online tool) incorrectly since April 2017. If HMRC is correct in a worst-case scenario going back 6 years we could owe as much as £150m, broken down between £110m of tax and £40m of penalties and interest.

4. Our Policy and assertion has been that we do not have the right to reject a substitute, HMRC's view is that we have a contractual right. The 'substitution' question is vital in determining the employment status of contractors.

5. In early April 2024 HMRC issued 'protective assessments' totalling £27m of tax covering 2017/18 to 2019/20 regarding this issue. These were issued as the early years can fall outside of a 6 year time limit if not assessed. HMRC started asking POL questions about this issue in June 2018 and we have continued to provide them information ever since, whilst maintaining the same approach to classifying contractors. As set out in previous RCC/ ARC papers should HMRC be proved to be correct we could owe as much £150m in

tax, interest and penalties. The assessments have been appealed and no further action will be required until agreement is reached with HMRC.

Corporation Tax – deductibility of compensation payments, running costs and treatment of DBT subsidy funding

6. The CT issue relates to the deductibility of costs associated with the schemes, both the compensation paid to affected Postmasters and the running costs of the schemes – HMRC contend that none of these costs are deductible as they were not incurred wholly for a business purpose, basing this on the 'oppressive' behaviour shown by POL regarding the affected Postmaster. In contrast to their view on the costs HMRC contend that all subsidy provided by DBT to POL to pay the compensation and any provided to cover POL's running costs associated with the schemes is incurred wholly for a business purpose and that is therefore taxable trading income. On 10 May 2024 we received a response to our sent to HMRC in October 2023, reaffirming their stance.

7. In earlier discussions HMRC estimated that there could be as much as £100m in CT owing as a result of this incorrect treatment, this figure was also quoted in the press in January of this year. However, we have worked with KPMG on building our tax model, covering reworking of the last 6 years of CT returns and based on following HMRC's stated position we have no tax owing, but possible penalties to pay for having filed returns with higher brought forward losses than would have been the case if we had applied HMRC's treatment from the outset. We are working on the complex calculations, but it would appear the worst-case figure is c.£5m to £8m. It is possible that HMRC could offer to suspend any penalties which would then be wiped from the record if no further errors arose. The tax position has been calculated using all reliefs available to POL, including brought forward historic losses and capital allowances, thus potentially creating future tax liabilities for POL.

8. DBT provided a funding offer letter to POL in December 2023 which contained several conditions. These included obtaining external assurance over the tax model, hence the KPMG review stated above, and that POL must cease its challenge with HMRC over the taxation treatment.

9. Following Board approval, POL have responded to accept the offer of funding, albeit with a number of additional requirements such as i) the ability to continue to discuss the details with HMRC, as the discussions to date have been at a high level and each scheme is different, and ii) that the acceptance of HMRC's views will result in future CT liabilities therefore funding needs to be assured for future costs and not just historical. Note future costs will arise both as a result of continued expenditure and funding for RM matters but also because POL is utilising its significant levels of taxation losses in order to reduce the liabilities. Current modelling indicates that by following HMRC's position we are likely to face a CT liability c£20m to £30m for 24/25 and c£5m to £10m for 25/26, however this is driven by RM forecasts for compensation in these years which will continue to be revised, and the estimates could therefore vary widely.

10. Following receipt of the HMRC letter we will be discussing the position further with DBT to confirm what additional subsidy we will require to pay the additional CT liability arising from DBT's subsidy funding provision to pay compensation to affected Postmasters. Applying the principles set out in HMRC's latest letter not all funding for all 'schemes' will

be deemed to be taxable trading income. We therefore will work through the detail and revise the model to take into account the complexities.

11. Once agreement is reached with HMRC and DBT we will submit revised CT returns for the affected periods. As a consequence of agreeing to this treatment we will need to pay quarterly instalments of corporation tax to HMRC as we will be deemed a 'very large' tax payer.

VAT - general

12. The primary VAT risk is to ensure that POL pays and claims the correct amount of tax. This year we have continued consolidating and refining our systems and processes for reporting VAT to HMRC. This is the second year in a row where we have not had to report a VAT error to HMRC.

VAT – liability of Postmaster services to POL

13. HMRC have questioned the VAT treatment of services supplied to POL by Postmasters in branches. HMRC asked whether it was correct that Postmaster remuneration should be split on a transaction-by-transaction basis, between all VAT exempt supplies and all taxable supplies. They have queried whether it would be more appropriate for it to be single supply of 'Postmasters Services'. If this was the case this single fee would be entirely subject to VAT, it would cost the business around £20m in additional irrecoverable VAT per year and cause thousands of Postmasters to exceed the VAT registration limit. We engaged KPMG to help us provide a robust response to HMRC which we sent on 2 February 2024. We await HMRC's reply.

Corporation Tax - CT returns 22/23

14. We have submitted the CT return for POL and POMS for 22/23. The CT return for Payzone is under final preparation and should be filed by the end of April. The Payzone delays have occurred due to the late signing of the Payzone financial statements, which were delayed until such point as POL was in a position to provide an appropriate Board approved letter of support.

Tax forecasting and maximising use of available reliefs

15. Historically our VAT recovery position remained very stable with little fluctuation in our VAT recovery rate on a year-on-year basis. It was consistently around 65% for 2016/17 to 2020/21. However, since the disposal of the telecoms business unit combined with the growth of Banking & Travel related income and the decline in Mails income our VAT recovery rate has significantly to around 50%. We expect that it will remain around 50% for 24/25 based on business income forecasts, representing a c.15% reduction on prior years and c.£8.25m of annual cost to operations in the form of additional irrecoverable VAT.

16. We have informed colleagues in FP&A of the possible impacts of the changing income profile and confirmed the amendment to the system set recovery rate of 50%, introduced in 23/24 is appropriate for 2024/25. This is sometimes referred to as iVAT (irrecoverable VAT) which is classed as 10%.

17. We expected to remain in a tax loss making position, despite making trading profits. However due to HMRC's stance on costs deductibility and subsidy receipts from DBT we

now expect to be in a CT paying position in 2024/25. Much depends on whether POL or DBT pay the compensation directly to affected Postmasters. If, as it appears likely at present, OC is administered directly by DBT this will reduce any future CT liability. However, as it appears likely that POL will pay the £75k flat compensation for HSS to affected Postmasters then this will create a large CT liability for us. We are working on modelling the scenario as we will then be required to pay CT each quarter to HMRC as a 'large taxpayer' and we will therefore require additional subsidy from DBT to cover this.

What other tax related issues should the RCC/ARC be made aware of?

Historic Settlement Scheme ("HSS") and Tax Top-ups (TTU)

18. In June 2023, in a welcome turn of events, HMRC announced an exemption for HSS tax top-up compensation payments. In 2021 we reached agreement with HMRC over which heads of loss were taxable and which were outside the scope. We have paid c£6m in tax withheld on compensatory interest and colleagues in payroll have paid PAYE and NICs for the same claimants. The TTU was established in August 2023 to start paying top ups to compensate claimants for the tax we withheld and paid to HMRC on their behalf. The formula, prescribed by DBT, sees claimants paid as if they had been taxed at 45% on their compensation, but then has a deduction to reduce the payments down ensure no-one has paid more than the equivalent of basic rate tax, addressing the unfairness point.

19. In late 2022/23 the RU team responsible for paying HSS compensation started to make some Interim Payments where a claim was under dispute. Unfortunately, they failed to report to the PM remuneration team and the Tax team that these payments were being made. The letters issued with Interim Payments made it clear tax was being withheld from payments, but no payment of tax was made to HMRC as the relevant teams responsible for reporting were unaware.

20. An exercise is underway to correct the position and disclose the sums to HMRC. This is being calculated by the TTU team as a part of their complex calculations work. The TTU team have obtained copies of all letters issued to claimants and are cross referencing these to the Integrity system, which is the single source of truth for claims. However, it does appear that this system does not contain all tax calculation details, therefore extreme care is being taken to update the system. We expect the tax due to HMRC to be substantial, in excess of £1m and we are likely to incur penalties and interest for not having taken reasonable care.

Governance and Tax controls

21. We continue to produce a quarterly tax summary report highlighting activity across all taxes which is circulated to the CFO, Head of Legal Services and the Group Chief People Officer and also disseminated more widely to senior parties in Finance and HR. We also hold regular meetings with Risk colleagues and sign off tax controls, every month through ServiceNow with supporting evidence uploaded into the system.

Tax team resource

22. As can be seen from the above there are several high profile tax issues under consideration at present. It is our desire to bring IR35 and the CT issue to a close and settle with HMRC in 24/25, albeit noting the timeframes are driven by HMRC. This will help provide more certainty to the business in terms of cost management.

23. Our Employment Tax Principal, Peter Gomersall, is retiring in May having already reduced his working hours. We have recruited a part time resource, Steph Dahl to replace Peter's part time work and will be seeking additional Employment Tax resource in the coming months to provide the expert knowledge we require to manage the issues and support colleagues across the business.

Tax Strategy – Annual Review

24. HMRC require that the POL Tax Strategy is reviewed, updated where required, and published on an annual basis. The initial strategy was presented to and signed off by the ARC in November 2017. The Tax team has reviewed the current strategy and have made minor amendments to ensure it remains fit for purpose and reflects our position and after sign-off will be published on our Corporate website and highlighted in a One News article.

25. The Tax Strategy is set out in Appendix 1.

Appendix 1 – Post Office Group Tax Strategy

This publication sets out the tax strategy of Post Office Limited and its UK subsidiary undertakings (referred to hereafter as the "Group" or "Post Office") for the financial year 2024/25, and in making this strategy available the UK Group is fulfilling its responsibilities under the Finance Act 2016, Chapter 24, Schedule 19, Part 2, Paragraphs 16 & 17.

This tax strategy applies to UK taxes applicable to the Post Office and its affiliated entities both in the UK and overseas. The document is ultimately owned by the Board of Directors of Post Office Limited ("the Board").

The tax strategy is reviewed annually, updated as appropriate and approved by the Board each January to cover the next financial year. The Board, along with assistance from the Group Finance teams, take ultimate responsibility for setting, monitoring and amending the strategy as required.

In summary, the Post Office is committed to:

- following all applicable laws and regulations relating to its tax activities;
- continuing to have an open and honest relationship with HM Revenue & Customs ("HMRC") driven by collaboration and integrity; and
- applying diligence and care in our management of taxes and ensuring that our tax governance is appropriate.

How the Post Office manages its tax risks

The Group's on-going approach to UK tax risk management and governance is based on the principles of reasonable care and materiality. The Post Office maintains on-going application of tax governance, including frequent risk metric assessments and the review of applications of strong internal control procedures in order to substantially reduce tax risk to materially acceptable levels.

As part of this governance, the Post Office has identified tax risks, which are maintained internally on risk registers, with their materiality being assessed based on a corporate risk matrix. The matrix then records the potential impact, subject to two contributory factors, the exposure if the tax risk crystallises and the relative likelihood of the risk crystallising.

Monthly review processes are carried out, based on the risk areas, and confirmation reports and evidence are logged in audit software. A quarterly tax issues report is then presented with significant / material issues to the Chief Financial Officer for their consideration, further discussion at Board level and with HMRC should the issue merit engagement of the tax authorities. Where decisions are deemed to be complex or have an element of uncertainty assistance from third parties may be sought to aid the Post Office's decision-making process.

Tax planning

Given that the Post Office is owned by the Government's Department for Business & Trade, it understands the importance of its transparent business operations.

The Post Office will not engage in artificial transactions the sole purpose of which is to reduce UK tax. As well as the above the Post Office will not engage in tax efficiencies if the underlying commercial objectives do not support the Group's position, or if the arrangements impact upon the Post Office's reputation, brand, corporate and social responsibilities, or future working relationships with HMRC.

Approach towards dealings with HMRC

The Post Office have always been and remain committed to maintaining integrity and transparency when dealing with HMRC. The Post Office underlines these principles by agreeing to:

- Accurately disclose all information required in correspondence and returns, and efficiently respond to communications as and when required. Where additional work is required, such as in the event of a disagreement, we will look to resolve this in the most professional and efficient way possible.
- Be open and transparent about decision-making, governance and tax planning, firstly by ensuring that it is liaising directly with our dedicated HMRC team and secondly by publishing our tax strategy easily accessible within the public domain.
- Ensure all interactions with HMRC are conducted in an open, collaborative and professional manner.

Signed

Kathryn Sherratt

Interim Chief Financial Officer and Senior Accounting Officer

(Updated April 2024)

18

POST OFFICE LIMITED
AUDIT RISK & COMPLIANCE COMMITTEE REPORT

Title:	Payment Practices Reporting Compliance	**Meeting Date:**	21 May 2024
Author:	Tom Lee, Group Financial Controller	**Sponsor:**	Kathryn Sherratt, Interim Group Chief Finance Officer

Input Sought: Noting

The ARC is asked to note Post Office Limited's compliance with Payment Practices Reporting requirements for the financial year ended 31 March 2024 ("FY23/24").

Previous Governance Oversight

- RCC - 7 May 2024

Executive Summary

Post Office Limited ("POL") has a statutory duty to file Payment Practices Reporting ("PPR") with Government on a bi-annual basis. Post Office Management Services Limited ("POI") and Payzone Bill Payments Limited ("PZ") fall outside the scope due to their size. Reports are still produced for POI as they use the same Purchase Order ("PO") system but are retained internally. The reporting includes payment policies, practices and performance. No changes have been made to the filing requirements in year.

POL has filed PPR as required for the past six financial years (FY18/19 to date) for the entities in scope. POL has controls in place within the Financial Reporting Controls Framework to ensure timely and accurate reporting. The reporting is shared with the Group CFO for POL and the CFO for POI to review and approve before filing or reporting internally. Note that a statutory director is required to approve the reporting for filing, therefore the CEO has formally approved the POL PPR reports for FY23/24. This report focuses on POL as the only reportable entity.

Payment performance has been consistently strong within POL. Paid to time rates averaged in excess of 90% for FY18/19 and FY19/20 with a slight drop to 85% in FY20/21 due to the introduction of a new procurement system, Web3. Following the bedding in of the new system the average paid to time rate increased to 95% in FY21/22 and was 93% in FY22/23. In FY23/24 the average paid to time rate was 95%, showing a slight improvement on the prior year. The primary drivers in late payments were late good receipting by the business (40%), changes to Purchase Orders / system issues (40%) and late receipt of invoices from the business into the AP team (20%). Additional training was rolled out at the start of the financial year to the business by the payment and procurement teams to remind colleagues of the importance of goods receipting and how to accurately do it in Web3, which appears to have had a positive impact.

Internal audit ("IA") completed a review over the process in Q4 FY21/22. The result was positive, with the findings being minor. Amendments, including some efficiencies and enhancements to the reporting process were made in FY22/23 as a result of the IA review. No further reviews have occurred in the year.

Questions addressed

1. What are Payment Practices Reporting requirements?
2. Has Post Office Limited Group been compliant?
3. What have the payment performance trends been to date?
4. What processes are in place to ensure compliance?

Report

Overview of payment practices reporting

1. Payment Practices Reporting ("PPR") is a statutory duty for companies, which exceed the size criteria as outlined in para 2, to publish information about their payment policies, practices and performance in relation to qualifying contracts for each reporting period in the financial year.
2. Companies are in scope for the financial year if on their last two balance sheet dates they exceed at least two of the following thresholds:
   i. £36 million turnover
   ii. £18 million balance sheet total
   iii. 250 employees
3. POL has been in scope for PPR for the last four financial years.
4. POI was in scope until end of FY20/21 when it dropped out due to a downturn in revenue.
5. PPR must be filed twice a year (April and October), with each report covering the previous 6 months.

Compliance to date

6. POL has filed PPR reporting since the rules came into place for financial years ending on and after 6 April 2017.
7. The payment performance statistics which have been reported to date are shown in Appendix 1. The table represents the percentage of invoices which have been paid within 30 days, 31 to 60 days or over 61 days for financial years.
8. The reporting includes policies and practices such as (i) standard payment terms (ii) changes to terms made in the reporting period (iii) dispute resolution processes. Appendix 2 shows a template of all of the required reporting information.
9. The reporting rules allow for different payment terms (i.e. more than 30 days) for different types of contract. However, POL primarily has standard 30-day terms across suppliers and therefore reports on this basis as standard.
10. POL has not received any Government correspondence in response to any PPR submitted to date.

Reporting trends

11. As shown in Appendix 1, the proportion of invoices paid within 30 days has been consistently high, remaining in excess of 90% in all periods, with the exception of H1 in FY20/21. The decline in that period was due to the impact of migrating to a new procurement system, Web3, with a move towards 3-way matching driving much of the decline as the business got used to goods receipting.
12. In FY23/24 the performance has increase to 95%, which may in part be due to increased training on the system and goods receipting at the start of the year.

13. Where payments have not been made within 30 days, the majority of the remaining payments are made within the following 30 days i.e. within 60 days.
14. POL has identified the main reasons for late payments as (i) late goods receipting, (ii) issues with purchase orders and system issues, including setup, errors and replacements, and (iii) invoices being shared with POL stakeholders instead of Accounts Payable and only being shared with Accounts Payable for processing once they are already overdue i.e. due process not being followed. In some cases invoices are also held back purposefully whilst negotiations are ongoing with suppliers, which impact the statistics also.
15. One of the IA findings in FY21/22 was that POL should determine a target level by which performance can be measured. Given the performance has been consistently high, this has not been a priority. However, the voluntary prompt payment code has a target of 95% within 60 days which POL has consistently achieved against and sets a good marker to continue to compare with. Although not formally a target we have achieved against this in year.

Processes in place to ensure accurate reporting

16. POL has controls in place within the Financial Reporting Controls Framework to ensure that it is compliant with the PPR rules and files accurate information on a timely basis:
    a. Bi-annual control whereby the Accounts Payable team prepare the PPR before the required deadlines. The reporting is reviewed by an Accountant outside of the Accounts Payable team to ensure independent assurance has been provided over the accuracy of the reporting.
    b. Bi-annual review of POL group entities against the scope criteria in section 2 to ensure POL is filing PPR for all required entities.
17. The final report is shared with the Group CFO for POL and the FD for POI Limited to review and approve before filing (where required). The email accompanying the report includes details of key trends in the period, as well as any changes to policies where applicable.

Appendix 1

POL	FY18/19		FY19/20		FY20/21		FY21/22		FY22/23		FY23/24	
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2
On time	96%	97%	94%	92%	85%	95%	96%	94%	94%	93%	95%	95%
1-30 days over	3%	1%	4%	6%	10%	5%	3%	4%	4%	4%	4%	3%
31+ days over	1%	2%	2%	2%	5%	0%	1%	2%	2%	3%	1%	2%

Appendix 2

Start Date of reporting period - per Govt notification

Day	27th
Month	Sept
Year	2023

End date of reporting period

Day	31st
Month	March
Year	2024

Payment Statistics

Average time to pay in days	31

A) % of invoices paid between day 1 and 30 (inclusive)	95%
B) % of invoices paid between day 31 and 60 (inclusive)	3%
C) % of invoices paid on or after day 61	2%
% of payments due in reporting period which have not been paid within agreed period	5%

Payment Terms and Qualifying contracts

Enter you standard payment period in days	30 standard terms
Describe your standard payment terms	Payment terms range from immediate payment to 30 days
Was there any changes in payment terms in reporting period	No
Enter the maximum contractual payment period	Maximum contracted payment term is 30 days or less

Dispute resolution process

Does your business offer e invoicing	No
Invoice document management	No
Does your business offer supply chain finance options	No
Can your business deduct sums from payments as a charge for being on the supplier list	No
Has your business deducted sums from payments as a charge for remaining on supplier list	No
Is your business a member of a code of conduct or standards on payment practises	No

POST OFFICE

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

19

Title:	Review of External Audit - post account approval	**Meeting Date:**	21 May 2024
Author:	Tom Lee, Group Financial Controller; Dan Ward, Head of Financial and Technical Accounting	**Sponsor:**	Kathryn Sherratt, Interim Chief Financial Officer

Input Sought: Discussion

The ARC is asked to **discuss** the external audit process ahead of the audit for the financial year ended 31 March 24 commencing in full.

Previous Governance Oversight

- None

Executive Summary

Management has undertaken a retrospective review of the audit process following the completion of the FY22/23 Annual Report & Accounts ("ARA"). The review encompassed internal management discussions on the overall process, including the ARA completion process and the associated PwC audit, as well as detailed discussions with PwC regarding the testing conducted and areas for improvement by both parties.

Regarding quality, no issues were noted, with PwC providing robust challenge throughout. Management is also satisfied with the level of knowledge and skills within the PwC team. The makeup of the team, especially at the senior level, is suitable for the size and complexity of the audit. Similarly, the minimal number of audit findings indicates that the processes on the POL side were robust in ensuring an accurate financial position was reported.

The main findings from the review were around efficiency with two key areas noted:

- POL management has a streamlined financial accounting team and this can create bottle necks and single points of failure. In order to address this, additional band 4 support has been reallocated to the audit for FY23/24, with an experienced financial and technical accountant assisting on the audit process to help with capacity.
- Remediation Matters provisions require a significant level of assessment both by POL management and PwC. The nature of the provisions means they can fluctuate considerably, and the level of support required can be significant. Having to re-audit the provision models as assumptions altered due to the elongated audit process created inefficiencies. In order to reduce the risk of re-auditing these provisions, management will assess the likelihood of a summer signing at the start of July. Should it not seem feasible, the audit of these balances will be halted until a revised signing timeline is agreed.

19

In addition to the above, the overall ARA creation process was complex and time consuming in the prior year and management is working on revising the approach to reduce the number of reviews by stakeholders and to identify ways to get better engagement from business stakeholders.

ARC is requested to reflect on and discuss the audit process, and the external auditor, ahead of the FY23/24 audit progressing in full. It should also be noted that the tender for the external audit has been concluded and a recommendation is being brought to ARC on this matter.

POST OFFICE

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

20

Title:	External auditor tender exercise – outcome and appointment	**Meeting Date:**	21 May 2024
Author:	Tom Lee, Group Financial Controller Antony Ray –Specialist Senior Procurement Manager	**Sponsor:**	Kathryn Sherratt, Interim Chief Financial Officer

Input Sought: Approval

The ARC is asked to **approve** managements recommendation to appoint PWC in the role of external auditor for the Post Office Limited group of companies ("POL"), with the appointment being for a period of 4 years, with the option to extend for a further 2 years, commencing with the financial year ended 30/3/2025 ("FY24/25"). The ARC Chair is requested to recommend the decision to POL Board for approval of appointment.

Previous Governance Oversight

- None

Executive Summary

The current external audit contract expires in October 2024, which covers the FY23/24 financial year. The incumbent auditor is PwC, who will have been in place for 6 years at the end of the contract. An FTS (Find a Tender) procurement exercise was undertaken using the Restricted Procedure. This approach was selected due to the complexity of the POL audit and the need to ensure respondents were limited to Tier One firms as defined by Financial Reporting Council (FRC), to ensure adequate quality of the audit firm.

Pre-market engagement activity was undertaken whereby all potential firms except for PwC advised they did not wish to participate in the procurement. The reasons were primarily linked to actual or potential conflicts of interests, due to other work undertaken or the ongoing Statutory Inquiry, and the risk associated with the audit (high risk client). PwC were therefore the only bidder in the process. A formal tender process was still undertaken, including bid submissions and presentations with associated scoring by POL assessors. PwC's bid was strong in all regards and the fee quote was competitive, with the estimate being in line with current year audit.

ARC are requested to approve PwC as the external auditor for a period of 4 years with the option to extend for a further 2 years, recommending this decision to Board. Finalisation of the contract will be undertaken by management and Board will be requested to delegate authority to Interim CFO for finalisation and signing of the contract.

Post Office Limited
Audit, Risk & Compliance Committee Forward Plan March 2024 - March 2025

Item	Origin of Request	Owner	Action Required	20/03/2024	21/05/2024	01/07/2024	18/09/2024	14/11/2024	27/01/2025	25/03/2025	Notes
STANDING ITEMS FOR PRESENTATION											
Welcome and Conflicts of Interest	Companies Act 2006 s.177	Chair	Noting	X	X	X	X	X	X	X	
ARC minutes from previous meeting	Terms of Reference para 67 & 72	CoSec	Noting & Approval	1/29/2024	3/20/2024	5/21/2024	7/1/2024	9/18/2024	11/14/2024	1/27/2025	
ARC Actions	N/A	CoSec	Noting	X	X	X	X	X	X	X	
RCC Summary	Terms of Reference para 17	RCC Chair	Noting	3/12/2024	7 May 2024	25 June 24	10 Sept 2024	12 Nov 2024	14 Jan 2025	11 March 2025	
Risk, Compliance & Internal Audit Update consisting: 1. Risk Report & Dashboard 2. Combined Compliance & Internal Audit Report	Terms of Reference para 10 - 16	Head of Risk, Director of Compliance, Head of Internal Audit	Noting	X	X	X	X	X	X	X	Compliance Report should contain an update on FCA proceedings. Risk report should include an overview of current and emerging risks as well as the Head of Risk's opinion on areas of concern etc (Committee Evalaution 2021). The Internal Update to every meeting should include updates on the plan whilst GLO assurance work is being undertaken.
5 minute break	Board/ARC Evaluation 2020/2021	CoSec	N/A	X	X	X	X	X	X	X	Any ARC meeting over 2 hours should have at least a five minute break.
WRITTEN RESOLUTION ITEMS											Unless agenda time allows, these items will be approved by written resolution sent in parallel with the meeting papers. They are therefore approved outside of the meeting.
Group Key Policies Review	Terms of Reference para 7 & 18	Director of Compliance (and/or Policy Owner)	Approval (for onward submission to the Board in some instances, where marked with an asterix)	(1) Procurement Policy (2) Health and Safety Policy	(1) Business Continuity Management (2) Cyber & Information Security (3) Whistleblowing/ Speak Up Policy (4) Employee Vetting Requirements Policy	(1) Financial Crime (2) AML & CTF (3) Anti-Bribery & Corruption (Incl Gifts & Hosp.) (4) Modern Slavery Statement (5) Conflicts of Interest Policy (6) Group Legal Policy	(1) Treasury (2) Business Change Management Policy (3) HMRC Fit & Proper Standards	(1) Risk -Board	(1) Protecting Personal Data Policy (2) Customer Complaints Policy - Board	(1) Health & Safety (2) Procurement (3) Document Retention Policy (4) Employee Vetting Requirements Policy	Each review and approval request is to include assurance and conformance testing to show the policy is operating effectively including details on exceptions/waivers and supporting evidence. All policies will be presented in one policy summary paper. Please check with Policy Compliance Manager before each meeting as this is subject to change and refer to the Group Key Policy Framework. Other policies on the Group Key list may be mentioned separately below due to their importance/requirement in the Terms of Reference and they will have separate papers. These are referred to in this list in brackets for completeness, but will not form part of the written resolution request). Policies must be presented as: - Minor changes - revised clean and track changed version - major changes clean revised version plus old existing version. NOTE: Other policies requiring RCC approval are in the RCC section of this forward plan as per the Group Key Policy Framework.
STANDING ITEMS FOR NOTING (NO PRESENTATION)											These items will not be presented to the Committee unless it is agreed otherwise. They are simply published and not discussed at the meeting. If there are any comments or questions, these are sent to CoSec. The comments/questions and answers are then appended to the minutes.
Procurement Governance & Compliance	September 2020 ARC/Procurement Policy	Procurement Director	Noting	X	X	X	X	-	X	X	
Post Office Insurance ARC update	Terms of Reference para 53	POI ARC Chair or POI Director of Risk & Compliance	Noting	X	X	X (presented)	X	X	X	X	This is noting only item with no presentation unless there is another POI item on the agenda.
Committee Forward Plan	Committee Evaluation 2021	Secretary	Noting	X	X	X	X	X	X	X	
		REGULAR ITEMS: EVERY SIX MONTHS, YEAR OR TWO YEARS (every year unless otherwise stated in notes column)									

Item	Origin of Request	Owner	Action Required	20/03/2024	21/05/2024	01/07/2024	18/09/2024	14/11/2024	27/01/2025	25/03/2025	Notes
Annual Report and Accounts , including: - ARA Cover Note & Draft ARA - Briefing Book - Accountable Person Report - Representation Letter - External Auditor Summary Report	Terms of Reference para 2, 3, 12, 42, 43, 44	CFO/Financial Controller	Noting & Approval (for onwards submission to the Board)	Plan to ARC for Decision	-	TBC	-	TBC	-	-	FY year end 31 March, deadline for filing 31 December
External Auditor Reappointment (next financial year), Fees & Scope of Engagement	Terms of Reference para 38	CFO/Financial Controller	Approval (for onwards submission to the Board)	-	-	This yr tender exercise closes June 2024	-	-	-	-	
Review of External Audit (post account approval) including independence, non-audit fees, qualifications, expertise and resources of the external auditor and the effectiveness	Terms of Reference Review 30/03/2021, Terms of Reference para 45, 48	CFO/Financial Controller/Chair	Discussion & Noting	-	X	-	-	-	-	X	This should be scheduled post approval of the ARA
External Audit Interim Update	Terms of Reference para 2, 42	External Auditors	Noting	-	-	X	-	-	-	-	
External Audit Plan	Terms of Reference para 41	External Auditors	Approval	-	-	-	-	-	X	-	
Financial Reporting Controls Environment	Terms of Reference para 2 and 10	Financial Controller	Noting	-	-	-	-	X	-	-	Annual item
Agreed Upon Procedures	Terms of Reference para 2 and 10	Financial Controller	Noting	-	-	TBC	-	TBC	-	-	To be included in Audit related papers going forward.
Accounting & Reporting Policies	Chair request 20/04/2021	Financial Controller	Approval	Plan	-	-	-	-	-	-	TL advised this was included in ARA updates
Annual Internal Audit Plan	Terms of Reference para 32	Head of Internal Audit	Approval	X	-	-	-	-	-	X	The Internal Update to every meeting should include updates on the plan whilst GLO assurance work is being undertaken.
Internal Audit Charter Policy	Terms of Reference para 31	Head of Internal Audit	Approval	-	-	-	-	-	-	-	**Every two years** To be next approved in May 2025 and then in May 2027. (Also on Group Key Policy List)
Internal Audit CoSource Independence Report including non-audit fees	Terms of Reference Review 30/03/2021, Terms of Reference para 35	Head of Internal Audit	Noting	X	-	-	-	-	-	X	Note: An external review of Internal Audit is required every 5 years. To date this has not been carried out. Should be added in due course.
Meeting with Internal Audit without management (pre-ARC meeting)	Terms of Reference para 35	Chair & Head of Internal Audit	N/A	-	-	-	-	-	X	-	
Meeting with External Audit without management	Terms of Reference para 47	Chair & External Auditors	N/A	X	X	X	X	X	X	X	A meeting at the end of each ARC from 16.05.23
Payment Practices Reporting Compliance	Company Secretary request due to director liability & s.172 reporting requirement	Financial Controller	Noting (no presentation, unless issue)	-	X	-	-	-	-	-	Moved to annual - May each year
Strategic Risk Management Review	Committee Evaluation 2021, Terms of Reference paras 13 & 14	Head of Risk	Discussion & Noting for onward submission to the Board	-	-	Defer to include funding impact upon strategic risks	-	-	-	-	Note: The Risk Policy requires the Board to have strategic oversight of Risk so this should also be submitted to the Board (see para 2.1 of the Risk Policy as approved on 7 January 2021 by the Board).

Item	Origin of Request	Owner	Action Required	20/03/2024	21/05/2024	01/07/2024	18/09/2024	14/11/2024	27/01/2025	25/03/2025	Notes
Post Office Insurance Deep Dive (covering risks, compliance & governance)	Terms of Reference para 53	POI ARC Chair or POI Director of Risk & Compliance	Noting	-	-	X	-	-	-	-	Annual Item in July. This is in addition to noting updates at every meeting (see above).
Technology Deep Dive	Terms of Reference para 10	Chief Information Officer/ Chief Information Security Officer	Discussion vs Noting	-	-	X	-	-	X	-	IT Controls should be twice a year at the January and July ARC meetings To cover: Joiners, Movers, Leavers, End User Management, Cyber Security
Cyber Security Update	Terms of Reference para 10	Chief Information Security Officer	Discussion vs Noting	X deferred from Jan CISO absent	X	X	-	-	X	-	Moved from Jan to March 2023 at Zdravko's request IT Controls should be twice a year at the January and July ARC meetings, for discussion vs noting - CS Email 24/08/2021
Mails Deep Dive	Terms of Reference para 10	Managing Director Parcels and Mails, Group Chief Commercial Officer	Noting	-	-	-	X	-	-	-	23/08/2021 - SK has agreed with CS that Mails Operational Controls will be biannual, in Jan 2022 and Sept 2022.
Banking Deep Dive	Terms of Reference para 10	Product Portfolio Director - Banking, Payments and Transactional Products, Group Chief Commerical Officer	Noting	-	X	-	-	-	-	X	23/08/2021 - SK has agreed with CS that Banking Operational Controls will be biannual in Jan 2022 and Sept 2022. January 2022 Deep Dive moved to May 2022. September 2022 Deep Dive moved to December 2022. Moved from December 2022 to January 2023
Identity Deep Dive	Terms of Reference para 10	Product Portfolio Director - FS, ID & Insurance	Noting	-	-	X	-	-	-	-	Annual Item.
Strategic Partner Risk & Failure Monitoring Deep Dive	Terms of Reference para 10	Strategic Partnerships Director	Noting	x	-	-	-	-	-	X	Annual Item
Data Protection Deep Dive	Committee Evaluation 2021	Data Protection Officer	Noting	-	-	-	-	-	X	-	16/02/2023: Deferred from Jan to March 2023. Deferred to September 2023. Deferred to November 2023. Deferred to January 2024
Business Continuity Update	Terms of Reference para 10	Business Continuity Manager	Noting	-	-	-	-	-	X	-	Annual Item.
Transformation Office Changes Update	Terms of Reference para 10	Group Chief Operating Officer/ Strategy and Transformation Director	Noting	-	X deferred from Jan as JW request	-	X	-	-	X	From 2023, this update will be twice a year in March and September.
Tax Update & Strategy	Terms of Reference para 18	Head of Tax	Noting & Approval	-	X	-	-	-	-	X	Annual Item -May
Corporate Insurance Renewal	Terms of Reference para 22	Group Treasurer	Approval	-	-	Group Insurance Renewal Options	Group Insurance Renewal Approvals	-	-	-	Annual Item. Insurance expires 31 October
Modern Slavery Statement	Terms of Reference para 18	Shaun Kerrison (Head of Postmaster Engagement)	Approval (for onwards submission to the Board)	-	-	X	-	-	-	-	Annual Item.
Risk Appetite Statements	Board Written Resolution 07/01/2021	Head of Risk	Approval	ESG	Change/ Strategy	Operational/ Marketplace & Brand/ Reputation	Legal & Regulatory	Technology, Information & Security/People	Commercial/ Financial/ Health & Safety	Governance	03/11/2022: Rebecca Barker to advise regarding scheduling these in. Annual review required. These statements are a work in progress and it has been agreed that they shoud be reviewed annually and where possible, at the same time as the Group Key Policy/ies to which the risk area relates is reviewed. This is a work in progress. More statements to be added to the plan in due course and review dates revised subject to alignment with Group Key Policy List. Rebecca Barker to advise which statements will be ready for each meeting. Presenter will be the GE member/SLT member for relevant area.
Fraud Risk	ARC Chair, August 2021	Group General Counsel, Head of Internal Audit, Group Compliance Director	Noting	-	-	X	-	-	-	-	

Item	Origin of Request	Owner	Action Required	20/03/2024	21/05/2024	01/07/2024	18/09/2024	14/11/2024	27/01/2025	25/03/2025	Notes
Legal Risk Review (non GLO/Starling)	Terms of Reference para 18 & 20	Group General Counsel & Group Legal Director	Noting	X	-	-	X	-	-	X	**Twice a year.**
Annual Money Laundering Report	Terms of Reference para 24, 25 & 27	Money Laundering Reporting Officer and Head of Financial Crime	Discussion & Approval	-	-	-	-	-	X	-	Approval of: recommendations in the Annual Report of the Money Laundering Reporting Officer for submisison to HMRC (regulator). Policy is approved separately in July.
Whistleblowing Policy & Review	ARC Meeting 30/03/2021, Terms of Reference B.23 & 24	Head of Central Investigations Unit	Noting & Approval (policy only)	-	X (Full Review & Policy Approval)	-	-	-	-	-	
Anti-Bribery & Corruption Report & Policy	Terms of Reference para 7 & 18	Money Laundering Reporting Officer and Head of Financial Crime	Noting & Approval (policy only)	-	-	X	-	-	-	-	
Remediation Unit Risk & Assurance Update	Email from Carla Stent 13/05/2022	Simon Recaldin (Historical Matters Director) and Ben Tidswell (POL NED and HRC Chair)	Noting - 15 mins	X was deferred from Jan	-	X	-	-	-	X	Twice a year in January and July. Commenced on 12th July 2022.
Climate risks and our approach under TCFD (Task Force on Climate-related financial disclosures).		Martin Hopcroft	Noting		X		X		X		Every second meeting. Commenced May 2024.
Postmaster Policies	N/A	Senior Operational Improvement Manager & Retail Engagement Director	Approval	(1) Network Transaction Corrections (2) Postmaster Onboarding (3) Postmaster Training policies (annual review)	(1) Network Cash and Stock Management (2) Network Monitoring and Branch Assurance (3) Postmaster Complaint Handling policies	(1) Postmaster Account Support (2) Postmaster Accounting Dispute Resolution policies	-	1. Postmaster Contractual Performance 2. Postmaster Contract Suspension 3. Postmaster Contract Termination 4. Postmaster Decision Review	-	(1) Network Transaction Corrections (2) Postmaster Onboarding (3) Postmaster Training policies (annual review)	These were new policies in 2020/21 and the Committee may, in due course, agree that they can be approved by the RCC but Chair has indicated that they should remain before the ARC for now. In March 2022, it was agreed to spread out the policy review dates. Full list: **September 2022:** Postmaster Account Support Postmaster Accounting Dispute Resolution **November 2022:** Network Monitoring and Audit Support Network Transaction Corrections Postmaster Complaint Handling **January 2023:** Postmaster Onboarding Postmaster Training Network Cash and Stock Management Postmaster Established Loss Recovery Policy **March 2023:** Postmaster Contractual Performance Postmaster Contract Suspension Postmaster Contract Termination Postmaster Termination Decision Review Postmaster Guide to Policies To include implementation
Committee Terms of Reference Review	Terms of Reference para 74	CoSec	Approval (for onward submission to Board if changes required)	-	-	X	-	-	-	-	
Committee Evaluation	Terms of Reference para 74	CoSec	Noting & Discussion (Approval of any actions)	-	Externally Facilitated Evaluation being undertaken	-	-	-	X (Review of Progress against actions)	-	Deferred as needs to be presented to Board prior. Board and Committee Evaluation is annual, but action progress is tracked every six months. This is scheduled for after the Board consideration of the results which normally happens each March.
ADHOC ITEMS											

Item	Origin of Request	Owner	Action Required	20/03/2024	21/05/2024	01/07/2024	18/09/2024	14/11/2024	27/01/2025	25/03/2025	Notes
Belfast Datacenter (Horizon) Disaster Recovery Post Test Briefing	Terms of Reference para 10	Head of IT Service Continuity	Noting only (no presentation)	-	-	X	-	-	-	-	Update was December 2022. Further update dates TBC. Note: Should link with dependencies e.g. SPM and is also part of IT Controls and should be flagged on Risk Register as required.
BEIS White Paper on restoring trust in audit and corporate governance	Finance request 19/04/2021, ARC request 18/05/2021	Director of Complaince	Approval / Discussion / Noting	-	-	X	-	-	-	-	Need to consider developing an assurance policy as a result of this. Presenters are Tom Lee, Christine Kirby, Johann Appel and Christian Spelzini. March 2022 is suggested date to provide Committee with plan to become compliant with new regime. This may move. June 2022 update: The BEIS whitepaper was delayed and only came out on 1st June Dec 2022 update: Item moved from Jan to March 2023 at per CK request
Data Governance (Framework)	RCC Meeting 04/05/2021/ ARC pre-meeting 06/05/2021	CIO/Head of Data Governance	Noting	-	X	-	-	-	-	-	Paper deferred to May 2023 ARC. Paper deferred to March 2023 ARC. Interim verbal update to November 2022 RCC. Deferred from July 2022 to Sep 2022 ARC then Sep to RCC and ARC Dec 2022 as per Matt and ZM request. This concerns an outstanding audit action but also wider data governance discussions which are happening around the business. A pre-ARC meeting agreed a single paper should be brought back outlining the current position, future plans etc. In due course, this is likely to be a regular item (twice yearly or annually and likely to encompass data protection in due course (see deep dive above)).
Mandatory Training: Status, changes and enhancements	ARC Meeting January 2023	Group Chief People Officer	Noting	X	-	-	X	-	-	X	Handed over from Anshu Mathur to Juliet Lang September and March each year
Speak Up Report	RCC Meeting May 2023	Group Legal Director	Noting	-	x	-	x	-	x	-	Every second ARC commencing July 2023
IR 35 Paper	NED request	Tom Lee/Andy Jamieson	Noting	x	x	-	-	-	-	-	
Documented list of SPMP risk and the parameters in which they will operate for releases especially with a PM lens.	NED request	Chief Transformation Officer/Programme Director (KG)	Noting	-	-	x					
Investigation action assurance	Via OW	Johann Appel	Noting		x	x	x				
NBIT Contract procurement controls ARC should have a role in providing assurance oversight	POL Board action	TBC	From POL Board action	-	-	X					
											HIDE BELOW WHEN PUBLISHING FOR ARC

POST OFFICE LIMITED
AUDIT RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Quarterly Speak Up Up-date	**Meeting Date:**	21st May 2024
Author:	Mair Haynes, Speak Up Analyst John Bartlett, Director of Assurance & Complex Investigations	**Sponsor:**	Sarah Gray

Input Sought: Discussion/Noting

Executive Summary

- This relates to Speak Up reports received during Q4 (1 January – 31 March 2024)
- Increased reports relating to conduct of POL senior managers are being received.
- Volumes of Speak Up matters reported have almost doubled from last quarter.
- Currently 15 Speak Up matters open. A higher proportion relate to POL staff, and the complexity and scale of these can be time and resource intensive.

24

Purpose

The purpose of this report is to provide ARC with an overview of Speak Up activity, the risks raised by those reports, and action taken to mitigate those risks.

Speak Up Reports this quarter

1. In this quarter (January to March 2024) twelve reports were made to the Speak Up team; almost double the number reported in the previous quarter (7), and are back up to previously seen average levels. 75% of these were reported by POL staff.
   1. Three allegations of ethics violation: one relating to a proposal of satisfaction scores in the colleague survey being used as metric for staff bonuses (this matter was closed when the metric was changed to measure participation); the other two included mention of the Inquiry and have both been passed for external investigation and will be reported on separately.
   2. Five reports relating to discrimination and / or bullying concerns: 'Dignity at Work' and 'Grievance' policies were shared where appropriate. Three matters have been closed and the reporters referred to the ER team in two instances. Further information is being sought in the remaining two matters.
   3. Two matters recorded as 'Out of Scope': one related to concerns around the relocating of a branch (closed and referred to Postmaster Onboarding and Contracts); the other related to a compensation request following an accident at work (agency branch) in 2021 (closed and advised to contact ACAS as postmaster was the employer, not POL).
   4. One report recorded as 'Other': concerns include feeling upset around previous postmaster terminations, and the cash declaration process; further details are being sought from the reporter.

v. One matter recorded as 'Modern Slavery': Limitations with the current Speak Up recording system means we are unable to amend Issue Types once they have been selected. This matter related to an assault within a branch some years ago which had been previously reported to the police which led to non-receipt of wages. Matter was closed and the reporter was referred to ACAS for advice regarding wages issues. This matter was also duplicated on our system as TBC which was closed immediately.

2. Eleven reports were closed during this period, with six of these referred to other departments / agencies to deal. In addition to those opened and closed this quarter and detailed above, four further matters were closed:

   i. One queried metrics used in the 2022/2023 STIP as it was believed certain elements were not communicated to all staff. People Team contacted and confirmation of metrics for that year shared with reporter.

   ii. One was a follow-up report of a matter that is already being investigated by the police, so this allegation was passed over to the police for action.

   iii. One was a report by a postmaster who had been arrested by police for his behaviour and was concerned a DSAR request had not been properly fulfilled. Liaised with Information Rights and matter closed.

   iv. One reported concern of how much time a colleague was 'available' on Teams.

24

3. There are currently 15 open Speak Up matters which have been passed to investigators who will report on these separately via the A&CI monthly MI.

Themes

4. *Ingrained culture and behaviour of senior leaders*: Reports of the same types of behaviour and involving the same departments continue to be received. Matters include dismissive behaviours, bullying, non-compliant recruitment processes and concerns around timescales for compensation payouts. Investigators have been assigned to these cases with enquires underway, upon completion of which, a report will be provided to Group Assurance with findings and recommendations.

5. *Mention of Inquiry:* The screening of the ITV drama 'Mr Bates v the Post Office' at the start of January prompted an increase in reporting of matters to Speak Up that made mention of the Inquiry. These matters range from triggering memories of experiences that happened in POL / branch many years ago, to reports providing details of alleged fraudulent compensation claims.

Challenges

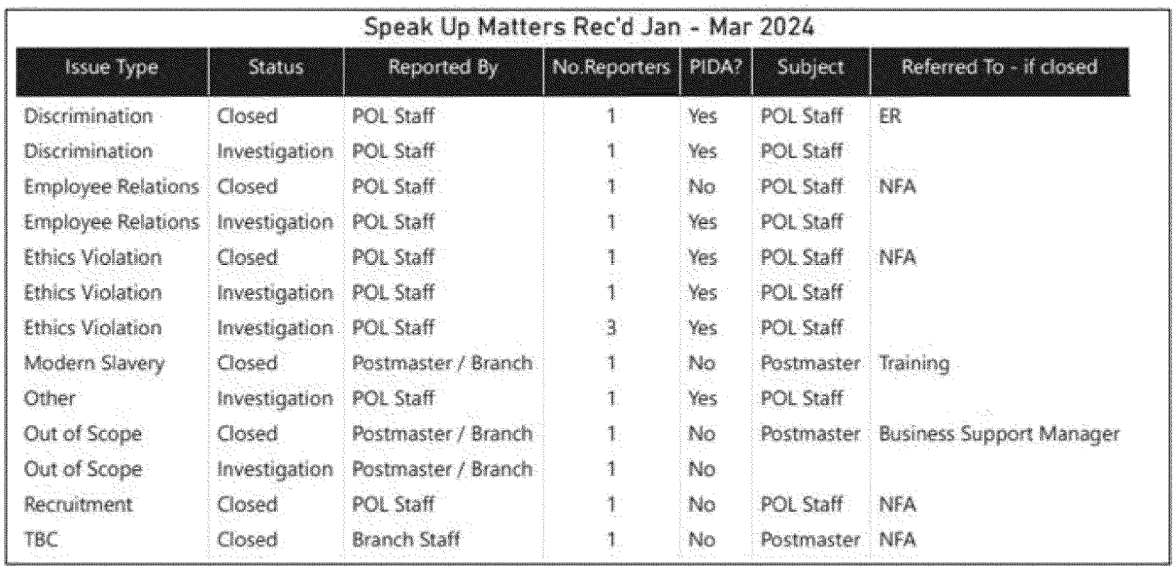
6. The continued lack of reliable, comprehensive reporting system with functionality for direct reporting, analysis, and data sharing hinders the effectiveness of the team in managing individual cases but also in thematic analysis. Difficulties around extracting

and maintaining data in the current stand-alone Speak Up reporting platform leads to potential duplication of work also being recorded elsewhere. Work is underway to identify a suitable system.

7. Sickness and secondment from within the Speak Up team to the investigation assurance part of A&CI meant an extended duration before some matters were closed. Recruitment for a replacement investigation manager is taking place.

24

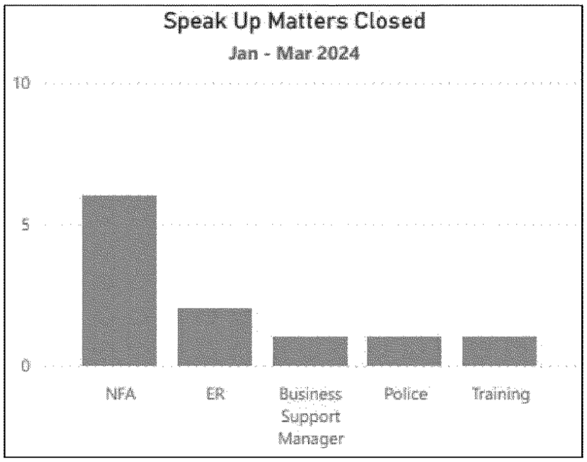
Appendix 1

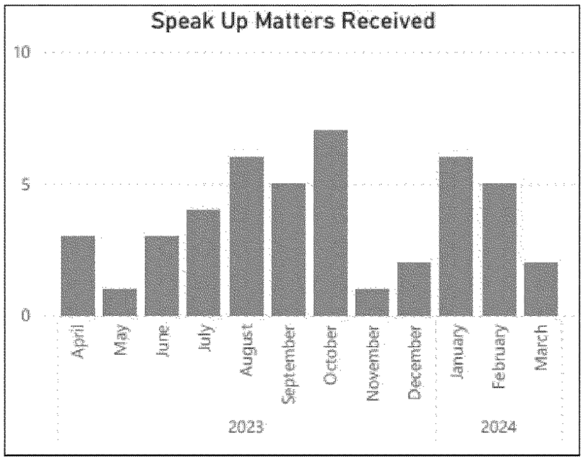


Speak Up Matters Rec'd Jan - Mar 2024

Issue Type	Status	Reported By	No.Reporters	PIDA?	Subject	Referred To - if closed
Discrimination	Closed	POL Staff	1	Yes	POL Staff	ER
Discrimination	Investigation	POL Staff	1	Yes	POL Staff	
Employee Relations	Closed	POL Staff	1	No	POL Staff	NFA
Employee Relations	Investigation	POL Staff	1	Yes	POL Staff	
Ethics Violation	Closed	POL Staff	1	Yes	POL Staff	NFA
Ethics Violation	Investigation	POL Staff	1	Yes	POL Staff	
Ethics Violation	Investigation	POL Staff	3	Yes	POL Staff	
Modern Slavery	Closed	Postmaster / Branch	1	No	Postmaster	Training
Other	Investigation	POL Staff	1	Yes	POL Staff	
Out of Scope	Closed	Postmaster / Branch	1	No	Postmaster	Business Support Manager
Out of Scope	Investigation	Postmaster / Branch	1	No		
Recruitment	Closed	POL Staff	1	No	POL Staff	NFA
TBC	Closed	Branch Staff	1	No	Postmaster	NFA

24


Speak Up Matters Closed
Jan - Mar 2024
NFA
ER
Business Support Manager
Police
Training


Speak Up Matters Received
April
May
June
July
August
September
October
November
December
January
February
March