POL00401629

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	10 September 2020
Time:	14.00 - 17.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chairman)	Johann Appel (Head of Internal Audit)
Ben Foat (Group General Counsel)	Mark Baldock (Head of Risk)
Amanda Jones (Group Retail and Franchise Network Director, Interim)	Jonathan Hill (Compliance Director)
Chrysanthy Pispinis (deputising for Owen Woodley)	Tom Lee (Head of Finance Financial Accounting and Controls)
Lisa Cherry (Group Chief People Officer)	David Parry (Senior Assistant Company Secretary)
Jeff Smyth (Group Chief Information Officer, Interim)	Rebecca Whibley (Assistant Company Secretary)
Julie Thomas (Operations Director)	Maxine Cross (Head of Reward and Pensions): Item 4
	Tony Jowett (Chief Information Security Officer): Item 5
	Joseph Moussalli (Programme Manager): Item 5
	Rob Wilkins (Cloud Services Director): Item 5
	Mark Dixon (Treasurer): Item 6
	Andy Bear (Locktons, Account Manager): Item 6
	Sarah Gray (Group Legal Director): Items 7, 8 & 9
	Tim Perkins (Head of Security, Safety & Loss Prevention): Item 10
	Daisie Jope (Head of HR - Organisation Effectiveness Project Lead): Item 11
	Barbara Brannon (Procurement Director): Item 12
Apologies:	
Nick Read (Group CEO)	
Owen Woodley (Group Chief Commercial Officer)	
Cathy Mayor (Finance Director)	
Dial In Details:	
Join Microsoft Teams Meeting GRO United Kingdom, London (Toll) Conference ID: 478 651 766# Pin (if applicable): 58042	

Time		**Item**		**Owner**	**Action**
14:00	1.	Welcome & Conflicts of Interest		Chairman	Noting
14.05	2.	Previous Meetings		Chairman	
		2.1	Minutes (13 July 2020)		Approval
		2.2	Action List		Discussion
14.10	3.	Combined Risk, Compliance and Audit Update			
14.10		3.1	Risk Report (dashboard)	Mark Baldock	Noting (onward submission to ARC)
14.25		3.2	Compliance Report	Jonathan Hill	Noting (onward submission to ARC)
14.40		3.3	Internal Audit Report	Johann Appel	Noting (onward submission to ARC)
14.55	4.	Pensions Assurance – RM Pensions		Maxine Cross	Noting (onward submission to ARC)

POL00401629

POST OFFICE LIMITED

15.10	5.	PCI-DSS and Cyber Security Update		Jeff Smyth/ Tony Jowett	Noting (onward submission to ARC)
		5.1	PCI-DSS	Jeff Smyth	
		5.2	Cyber Security	Tony Jowett	
		5.3	Joiners, movers, leavers	Tony Jowett	
15.25	6.	Corporate Insurance Renewal 2020/21		Mark Dixon/ Andy Bear	Noting & Approval (onward submission to ARC)
15.35	7.	Law & Trends Update		Ben Foat/ Sarah Gray	Noting (onward submission to ARC)
15.45	8.	Annual Legal Risk Review (excluding GLO/Starling)		Ben Foat/ Sarah Gray	Noting (onward submission to ARC)
15.55	9.	Contract Management Framework		Ben Foat/ Sarah Gray	Noting (onward submission to ARC)
16.05	10.	Update on Postmaster Accounts		Tim Perkins	Noting (onward submission to ARC)
16.15	11.	Deepdive: Successfactors		Lisa Cherry/ Daisie Jope	Noting (onward submission to ARC)
16.35	12.	Policies for Approval: Late Paper Inclusion: Procurement includes: • Procurement Policy • Appendix A Guidance on Sub-Threshold Awards • Appendix B Pren Guidance • Appendix C Purchasing Process 1. Summary Paper 2. Contract Execution 3. Vulnerable Customer 4. Physical Security 5. HMRC Fit and Proper Standards		Jonathan Hill Barbara Brannon	Noting (onward submission to ARC)
16.50	13.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 22 September 2020		Chairman	Noting
16.55	14.	Any other business		Chairman	Noting
Next RCC Meeting: Thursday 12 November 2020 at 14.00 to 17.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ					

POL00401629

2

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance Committee ("RCC") meeting held via Microsoft Teams
on 13 July 2020 at 14:00

Present:	Alisdair Cameron (Chair) (AC)	Group Chief Financial Officer	
	Ben Foat (BF)	Group General Counsel	
	Amanda Jones (AJ)	Group Retail and Franchise Network Director, Interim	
	Lisa Cherry (LC)	Group Chief People Officer.	
	Jeff Smyth (JS)	Group Chief Information Officer, Interim	
	Julie Thomas (JT)	Operations Director	
	Chrysanthy Pispinis (CP)	Post Office Money Director, Post Office	
In Attendance:	Johann Appel (JA)	Head of Internal Audit	
	Mark Baldock (MB)	Head of Risk	
	Jonathan Hill (JH)	Compliance Director	
	Tom Lee (TL)	Head of Finance, Financial Accounting and Controls	
	David Parry (DP)	Senior Assistant Company Secretary	
	Tony Jowett (TJ)	Chief Information Security Officer	Item 4
	Joseph Moussalli (JM)	Programme Manager, Project Managers and PMOs	Item 4
	Rob Wilkins (RW)	Cloud Services Director, MI, Data Strategy & Analytics	Item 4
	Tim Armit (TA)	Business Continuity Manager	Item 5
	Tim Perkins (TP)	Head of Security, Safety & Loss Prevention, Loss Prevention	Item 7
	Maxine Cross (MC)	Head of Reward & Pensions, Reward & Pensions	Item 8
	Sarah I Gray (SIG)	Group Legal Director	Item 9
	Andy Kingham (AK)	Head of Network, Retail Network	Item 10
	Sally Smith (SS)	Head of Financial Crime	Item 10
Apologies	Nick Read, Group CEO		
	Owen Woodley, Group Chief Commercial Officer		

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

POL00401629

2

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

POL00401629

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

DRAFT

POL00401629

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

POL00401629

2

	The team has now completed a review of contracts not previously remediated or de-scoped during the original GDPR remediation programme, identifying 7 key contracts as high risk including: • CWU • Unite • Fujitsu Telecoms • Global Payments • OH Assist • RAPP • Selenity.	
6.2	Work is underway to support the contract owners, however the Committee remains concerned that other high risk contracts may be identified following programme completion. The GDPR Update paper was **NOTED for onward submission to the ARC.**	
7.	**Suspense Accounts**	
7.1	BF and TP presented the Suspense Accounts report. BF explained that KPMG had been commissioned to review whether POL has profited from money held in suspense accounts, following longstanding allegations pre and post GLO.	
7.2	A review of current practices has now been completed and identified four suspense accounts currently in operation. These suspense accounts contain money that is: (1) Either not taken to a profit and loss account; or (2) Relates to unmatched transactions due to customers (not Postmasters); or (3) Relates to surpluses rather than shortfalls.	
7.3	TP remarked that no money has been identified as being taken for profit, and that the team would be implementing KPMG's suggested recommendations over the course of the year. It was noted the review did not cover the historical operation of the suspense accounts, which the Chair requested be investigated.	**Action: TP**
7.4	The paper was **NOTED for onward submission to the ARC.**	
8.	**Pensions Assurance**	
8.1	MC presented the Pensions Assurance paper. She advised that ahead of the POL purchasing its share of the Royal Mail Pension, the project had identified a number of IRRELEVANT IRRELEVANT	
8.2	IRRELEVANT IRRELEVANT An internal audit has also been commissioned to understand why this has not been previously identified, and to ensure that any lessons are learnt.	
8.3	BF highlighted to the Committee that the POL's directors may wish to make a report to the regulator, and that they would be entitled to obtain their own independent legal advice which could be arranged through the legal team. The Committee discussed and recognised the potential for future litigation and regulatory fines (which should not be underestimated), and noted that the legal advice received had strongly indicated that no report should be made at this stage, until the scale of issue was known. MC was reminded that the potential for litigation should not be underestimated.	
8.4	The paper was **NOTED for onward submission to the ARC.**	
9.	**Law and Trends Update**	
9.1	SIG presented the Law and Trends update paper.	
9.2	She explained the purpose of the paper was to highlight any future legislation and or regulation that may impact POL, bringing the following to the Committee's attention: • Covid 19 Employment Legislation Updates. • ATM Additional Business Rates Update. • Public Sector Bodies (Websites and Mobile Applications) (No.2) Accessibility Regulations.	

POL00401629

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

DRAFT

POL00401629

Post Office Limited Risk and Compliance Committee Actions
Updated: 04.09.2020

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
RCC Meeting 13.07.20					
3.5 Compliance Report	**Fairness** – the Telco team was asked to consider ways to reduce the number of 'vulnerable customers' and to revert to the Committee with a statement/plan for November.	Meredith Sharples	November	On-going	Open
7. Suspense Accounts	It was noted the review did not cover the historical operation of the suspense accounts, which the Chair requested be investigated.	Tim Perkins	September	The work with KPMG remains on-going and a full report will be provided in November.	Open
RCC Meeting 06.05.20					
3.15 Combined Risk, Compliance and Audit Update: Internal Audit	**Internal Audit reviews completed**: The Fit & Proper policy was also being updated and LC was asked to ensure that HR were involved in this update	LC	*Please provide suggested due date*	LC has spoken to JT and an update will be provided in September.	Open
RCC Meeting 14.03.20					
6.6 Annual Legal Risk Report 2019/20	The Committee questioned whether these examples had been flagged to the Committee or ARC before? [Post meeting note – these issues have not been raised previously to the Committee or to ARC.]	DP/RW	~~06/05/2020 13/07/2020 (RCC Meeting)~~ 10/09/2020	Update: 10/09/2020: a legal risk review paper (non-GLO and Starling) will be presented twice a year to RCC and ARC in September and March respectively. --- These issues have not been raised previously to the Committee or to ARC. Update 06/05/2020: The issues being flagged to the RCC or ARC was questioned as to its context. It was requested that more information was provided as it was not enough to simply say that it was not raised. Update 21/05/2020: Context: This action was in respect of Competition Law and the acquisition of PZBPL – *"Following the acquisition of Payzone Bill Payments Limited (PZBPL) , the legal team has provided advice/guidance on sharing commercially sensitive information*	Recommend for closure.

POL00401629

Post Office Limited Risk and Compliance Committee Actions
Updated: 04.09.2020

				between POL and PZBPL, conflicts of interest, and going to market service offerings. Examples of issues have included PZBPL management (POL staff members) seeking to make decisions on behalf of POL rather than PZBPL and requests from PZBPL for confidential information held by POL in breach of confidentiality obligations to a mutual client. "	
RCC Meeting 14.01.20					
10.6 - Money Laundering Reporting Officer (MLRO) Annual Report	BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC.	SS/JH	*Please provide suggested due date*	09/07/2020: HMRC are not conducting meetings at present due to Covid, but Sally has chased. Delayed due to scheduled meetings being postponed. Update from Sally: We have been unable to arrange the meeting with Ben and HMRC as yet – our new Supervisor was appointed end February, but since Covid-19 lockdown, HMRC are not undertaking any Compliance activity, and clearly we are not able to meet. If the current situation continues, I will see if we are able to sort out a meeting for Ben via Teams.	Open
RCC Meeting 07.11.19					
3.2 Supplier Contracts out of Governance	SSK – retail lead team decision required to ensure project does not stall.	Kathryn Sherratt/ Nick Wade /CM/Marketing	*Please provide suggested due date*	In progress – subject to PSG funding. 'On hold' given the change re-prioritisation. OJEU process is being finalized to demonstrate progress since action was set. The SSK Procurement Project is on hold at present. This work will now form part of NEO Work Package 5, which is due to report to Board in June and July on Network Shape and Formats and Propositions respectively. NEO WP5 will return to Board in September with the Technology part of the work stream, the direction from which will form part of the Procurement. The project will return to PRB to resume work following the September Board.	Open

POL00401629

Post Office Limited Risk and Compliance Committee Actions
Updated: 04.09.2020

3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	~~SH~~ JS / Marketing	*Please provide suggested due date*	In progress – subject to PSG funding.	Open
5.3 Cyber Security	A major incident test be completed with findings reported to the Committee.	TJ/JS	~~January 2020~~ 13/07/2020 (RCC Meeting)	The test was scheduled for March but was interrupted by preparations for COVID – to be rescheduled. Update to be provided in Cyber Security update paper. Update 06/05/2020: JS to provide an update.	Open

Strictly Confidential

POL00401629

Central Risk Dashboard

RCC & ARC

10 September 2020

Strictly Confidential

POL00401629

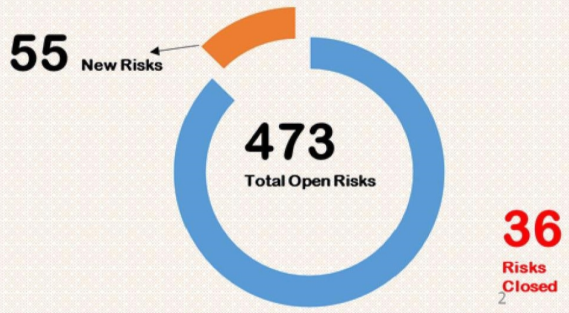
1. Summary

Summary

As @31/8 the Post Office has **473** open risks across the 3 level hierarchy, a net increase of **19** since the last reporting period. Key points to note include:

- **55** new risks identified at the local level – primarily in the Commercial (**20**) & IT space.
- **36** risks closed - primarily as a result of a review of risks across the business.
- Assimilating COVID-19 risks within BAU risk management.
- Emerging risks around Brexit – impact analysis underway which may see some risks activated in the next reporting period.
- Work continues on risk appetite and KRI development – illustrative position included within this reporting pack – clear need to put these structures in place as majority of active risks continue to be treated even though it may prove they are trending within appetite.
- Strategy: need to consider the extent to which current risk profile needs review as a result of the launch of a refreshed Post Office strategy.

Risk Profile churn



Central Risk Review

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

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

Strictly Confidential

POL00401629

2. Enterprise Level: Summary

Summary

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

Given their strategic nature enterprise risks do not see significant change in ratings month on month albeit **7** of these (i.e. Operational and Change) has seen a slight increase over the period. This is in part because Central Risk are providing increasing challenge around understanding how movement and churn at the lower levels have a material impact at the enterprise level.

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

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

Enterprise Risk Heat Map

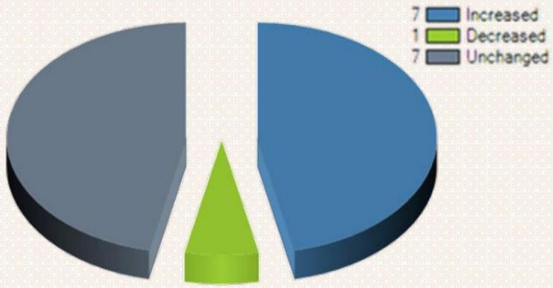


Key Risks

Key enterprise risks include:

- **Commercial:** Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market.
- **COVID 19:** Risk that the Post Office business employees and postmasters are adversely impacted by the spread of the COVID-19 virus and wider associated socio-economic activity.
- **Legal:** Risk the Post Office is unable to comply with legislative and regulatory changes.
- **Financial:** Risk that the Post Offices has insufficient funding and/or uncontrolled costs in the short-, medium and long-term.

Enterprise Risk rating change



POL00401629

3. Enterprise Level: Key Risks

Risk #	Risk Owner	Enterprise Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Date]	Latest Residual RAG (I/L) [Date]	Trend	Actions/Mitigations	Target RAG (I/L)
12	Owen Woodley	**Commercial:** Risk the Post Office Commercial proposition is unattractive because the existing products are too complex or confusing, new product are cost ineffective, unable to be scaled and unattractive to the market.	(4/3)	(4/4)	(4/4)	⇨	• PO Strategic review - Commercial strategic review of what does the business look like after we come out of Covid 19 crisis is currently underway to identify what Markets are critical for Post Office and the supporting operational functions and dependencies to support this, including key systems, staff, third parties, polices and operational hub (Board review on 2 day away day in 7/2020 and outcome 9/2020) • PO Digital Strategic review - Develop a revised Post Office Digital strategic plan (9/2020) • Commercial Policy & Procedure review - Undertake policies and procedures review to ensure they remain adaptive and flexible to long-term (9/2020)	(3/3)
84	Al Cameron	**COVID 19:** Risk that the Post Office business employees and postmasters are adversely impacted by the spread of the COVID-19 virus and wider associated socio-economic activity.	(4/4)	(4/4)	(4/4)	⇨	• Partner stability Regular financial monitoring of Commercial Partners • Network Strategy Reflect impact of coronavirus closures in Network Strategy • Postmaster Proposition – Development of attractive and flexible propositions that can be deployed quickly	(3/3)
18	Ben Foat	**Legal:** Risk the Post Office is unable to comply with legislative and regulatory changes.	(5/3)	(5/3)	(5/3)	⇨	• GLO – Programme remains ongoing to identify and resolve with all impacted postmasters. (ongoing) • Contract Management - S2S in place to manage contracts, further work required to understand scope, work with procurement underway. (12/20) • Compliance – Policy review manager undertaking review of Policies across the business. Work remains ongoing to review controls to ensure adequacy (TBC) • Appetite & KRI – work has been carried out with Central Risk to review the RAS for Legal & Compliance (pending review with Governance) to ensure risks as being managed adequately and are monitored effectively. View to refresh and approve for Nov RCC.	(3/2)
20	Al Cameron	**Financial:** Risk that the Post Offices has insufficient funding and/or uncontrolled costs in the short-, medium and long-term.	(5/3)	(5/3)	(5/3)	⇨	• PO Strategic review (Project NEO) - Commercial strategic review of likely post-COVID-19 environment to determine optimal operating requirements and associated required funding. • Cashflow monitoring - weekly budgeting implemented; industry cashflow impacts of COVID pandemic being monitored.	tbc

[redacted]

POL00401629

4. Intermediate Level: Summary

Summary

The Post Office has **72** intermediate risks of which **4** are rated as Critical, **24** Very High and **42** high.

42% of these risks has seen an increase in their current risk rating in the last reporting period with 31% remaining unchanged. This level of relative volatility is primarily the result of increasing Central Risk scrutiny and challenge along with the business re-articulating and refocusing some risks as accountability becomes clearer.

15 intermediate risks have been categorised as Commercial. These include risks associated with Banking Services dependency, existing product simplicity and the relevance of new products. **8** intermediate risks are Operational which including risks around the fragility of multiple partners, postmaster remuneration and maintenance of Network numbers.

Intermediate Risk Heat Map



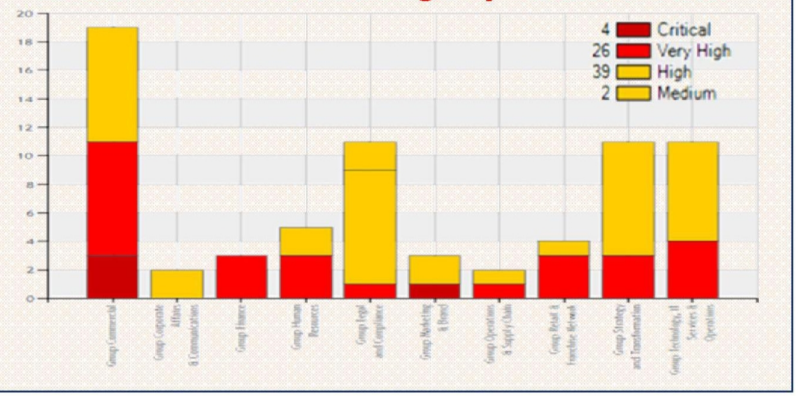
Key Risks

Key risks include;

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

The ongoing management of many such risks will be shaped by final decisions on the Post Office's (refreshed) Strategy and associated workplan

Intermediate Risk Ratings by Business Area



Strictly Confidential

POL00401629

5. Intermediate Level: Key Risks

Risk #	GE Risk Owner	Intermediate Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Date]	Latest Residual RAG (I/L) [Date]	Trend	Actions/Mitigations	Target RAG (I/L)
70	Owen Woodley	**Government Services:** Risk the Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) may reduce over the short-, medium- and long-term.	(4/5)	(4/5)	(4/5)	⇨	• Reviewing a faster roll out of the tablet services to ensure present and ready for the travel bounce-back period. • Discussing with marketing an awareness campaign to put PO services front of mind, emphasising the ease and certainty that comes through transacting with us . • Regular meetings with Government Departments in the role PO can play.	tbc
64	Owen Woodley	**Digital Income:** Risk the on-line products and services generate a reduced income level compared to comparable physical products and services.	(4/3)	(4/4)	(4/4)	⇨	• Given the existing Covid-19 crisis, a Commercial review of what does the business look like after we come out of this crisis is currently underway to identify what Markets are critical for Post Office and the supporting operational functions and dependencies to support this.	tbc
53	Owen Woodley	**Telco Dependency:** Risk Post Office has limited influence on Fujitsu's T&C's (or ability to exit) therefore undermining performance and change affordability.	(4/4)	(4/4)	(4/4)	⇨	• Given the existing Covid-19 crisis, a Commercial review of what does the business look like after Post Office come out of this crisis is currently underway to identify what Markets are critical for Post Office and the supporting operational functions and dependencies to support this.	tbc
4	Emma Springham	**Customer Demand:** Risk the existing and emerging requirements of Post Office (new and existing) customers across the various sectors are not met.	(5/3)	(5/3)	(5/3)	⇨	• Workstreams underway to develop plans and align with Project NEO objectives.	tbc

Strictly Confidential

POL00401629

6. Local Risk Level: Summary

Summary

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

This work is ongoing but current data shows (as at end of 8/2020) we have **386** open Local Level risks. This is a **-10** net reduction since 7/2020 (**10** new risks raised and **20** closed in monthly reporting period). The bulk of these low level risks have been categorised as Commercial (**64**), Operational (**55**) and Legal (**70**). The latter cover risks around potential non-compliance across various regulations (AML, ABC, vehicle safety, environment etc). There has also been (**28**) IT local risks articulated around specific IT components reaching 'end of life'. IT have an emerging risk: Fujitsu datacentre failed over the Bank Holiday weekend, the complete environment was failed over and brought up on DR and restored again onto production with only minimal interruption to BAU, so there's confidence now on the shutdown / restore activities.

Central Risk are proactively liaising with Business Risk Leads to ensure local risks are correctly articulated, rated and categorised. This may see some movement in numbers and the shape of the profile at this local level in coming weeks. Target ratings in many cases await the outcome of the risk appetite and KRI work.

Local Risks Heat Map

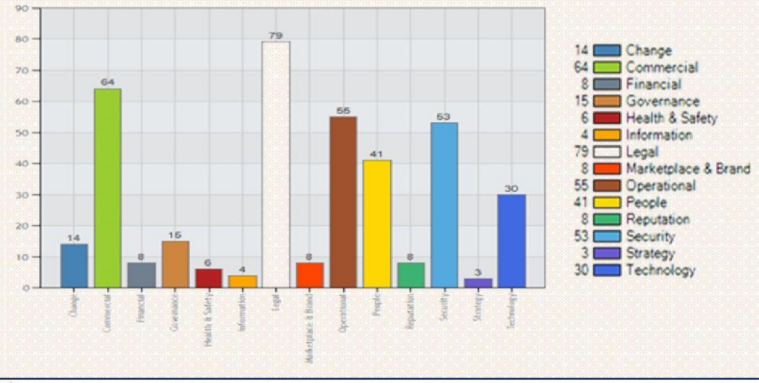


Key Risks

There are 3 Local Level risks whose current rating is Critical (20) namely

- Industrial Action: Risk the Post Office Commercial proposition is unattractive because existing products are too complex or confusing, new product are cost ineffective, unattractive to the market and/or unable to be scaled.
  Key mitigation include refreshed IR Framework, direct comms to Field teams and employees, and regular review of IA contingency plans
- Health & Safety: Risk Post Office business employees and postmasters are adversely impacted by the spread of the COVID-19 virus and wider associated socio-economic activity. Ongoing mitigation include provision of PPE equipment, maintenance and monitoring of Government guidelines of maintaining safe distance between customers/staff and monitor existing workplace H&S hygiene measures
- Impact of COVID-19 on Change Portfolio: Risk there is insufficient change funding available to deliver planned change activity. Key mitigations include re-prioritisation of the change portfolio (and a recalibration following the launch of a refreshed Strategy) and discussion with UKGI re LT funding as part of the Government's comprehensive spending review.

Local Risks by Category



Strictly Confidential

POL00401629

7. Local Risks: Key Risks

Risk #	GE Risk Owner	Local Risk Title	Inherent RAG (I/L)	Previous Residual RAG (I/L) [Date]	Latest Residual RAG (I/L) [Date]	Trend	Actions/Mitigations	Target RAG (I/L)
183	Amanda Jones	**Industrial action - Directly Managed Branches (DMB):** Risk of Industrial action because of proposed changes to the DMB network.	(3/5)	(3/3)	(4/5)	↑	• Dispute Resolution Programme – programme in place including GOLD teams to mitigate as conversations remain ongoing with the CWU to ensure transparency.	tbc
178	Amanda Jones	**Health and Safety Breach - Branch Network:** Risk of harm or breach of regulatory requirements.	(5/4)	(5/4)	(5/4)	→	• Response to COVID-19 pandemic – PPE issued and available to buy, branch communications issued. • Health & Safety activities – ongoing to annual plan	tbc
426	Alistair Cameron	**Mental and physical health and safety:** Risks through crime such as violence and hate crime	(5/4)	(5/4)	(5/4)	→	• Trauma support – EAP and line manager support in place • Hate Crime Campaign – to be issued	tbc
46	Dan Zinner	**Impact of CV19 on Change Portfolio C-19:** As a result of CV19's impact on trading profit and the cost of reacting to CV19, there is a risk that there isn't enough change funding available to deliver PO's planned change activity.	(4/5)	(4/5)	(4/5)	→	• Identify projects with Regulatory impact and complete assessment as part of GE options review - end April. • Continue to manage flexibility of Post Office cash flows with UKGI - Ongoing via activity led by Finance • Prioritise Change activity.	tbc

Strictly Confidential

POL00401629

8. Change Risks[1]

	Previous Month RAG Status	Current Month RAG Status	Summary Points
Overall	Amber	Amber	Overall Portfolio status remains at Amber. The draft four year plan was reviewed at the July Board, with an updated plan being submitted late August, this will determine the scale and shape of our future change portfolio to help achieve our strategic ambitions.
Benefits	Red	Red	Benefits achieved in P4 were £6.5m and £23.4m Year to date, YTD performance is £2.8m below budget, driven mainly by Insurance projects. Status maintained at Red as benefit forecasts have been reduced and full year benefits budget is at risk due to CV19 /trading and changes to programmes which bring benefits e.g. DMB and OE, due to sensitivities around these programmes.
Investment	Amber	Amber	Investment spend in P4 was £10.7m and £43m Year to date, this was lower than budget mainly due to HR programmes being delayed to later in the year.
Risk	Amber	Amber	The number of Gold & Platinum projects reporting a Red risk status remains at 2 with an inclusion of Project Assurance in this report and Paystation Refresh that was reporting Red for Risks in P3 has change to Green.
Delivery	Amber	Amber	Delivery remains Amber, several major programmes are progressing through closure and People programmes restated as planned

Portfolio	Previous Month RAG Status	Current Month RAG Status	Summary Points
Commercial Products	Amber	Amber	Majority of projects have an overall Amber status (Payzone, British Gas and Digital Identity, all reporting red in some areas)
Efficient Central Support	Red	Amber	Two of the six projects (GDPR and original GLO project) both reporting Red in some areas..
IT Platform Enablement	Green	Green	Four of the seven projects reporting Green overall. Back Office Transformation, Horizon Integration Hub and Fujitsu negotiations (Everest) are currently in the closure process
Mails	Red	Red	Mails Strategy is the only live gold /Platinum project and is reporting Red
Operations	Amber	Amber	Branch Hub reporting Green, Post GLO Ops & Contract improvements and Fit and Proper reporting Amber
Organisational Effectiveness	Green	Amber	Three of the five projects reporting Green overall, Project Assurance is additional this month and is reporting a Red for Risk and Overall,
Postmaster & Network	Amber	Amber	DMB Strategy reporting Green across all areas, Network Dev reporting Amber

[1] UKGI monthly report (P4 – 7/2020)

POL00401629

Central Risk

*Legal, Compliance & Regulation Risk Appetite Statements & Key Risk Indicators (KRI) Dashboard [**Draft**]*

10 September 2020

Strictly Confidential

POL00401629

Executive Summary

Background

In 6/2020 GE commissioned Central Risk to update the Post Office's corporate risk appetite statements, develop supporting Key Risk Indicators (KRIs) and pilot the approach in Operational, Technology & Security and Legal Compliance & Governance (LCG).

Central Risk have focused initially on LCG through a desk-based risk review, the completion of a simple questionnaire and a series of detailed 121 meetings. We have pulled together a suite of draft LCG appetite statements, supporting KRI's and indicative thresholds. These **are still in draft** as they will still be subject to GE, Board, ARC approval. They have been included in this pack to give an illustration of our emerging approach and how the individual GE member, supported by their Risk Lead and Central Risk, can use it to regular monitor performance against their risk appetite and keep within approved tolerances.

Illustrative Findings

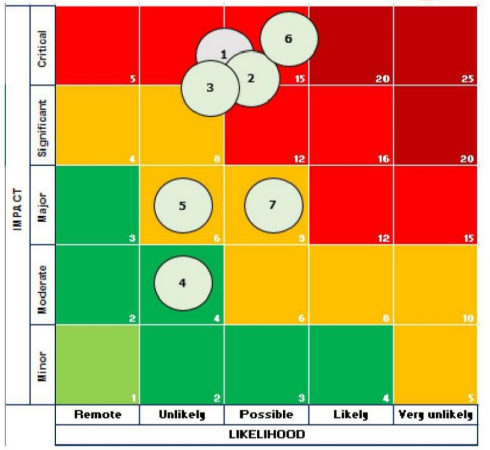
Central Risk's findings are that LCG has **1** enterprise and **7** linked intermediate risks split into **5** groups. Each group has a defined risk appetite (which applies to all the risks within that group) and a range of supporting associated KRIs. The groupings and indicative appetites are

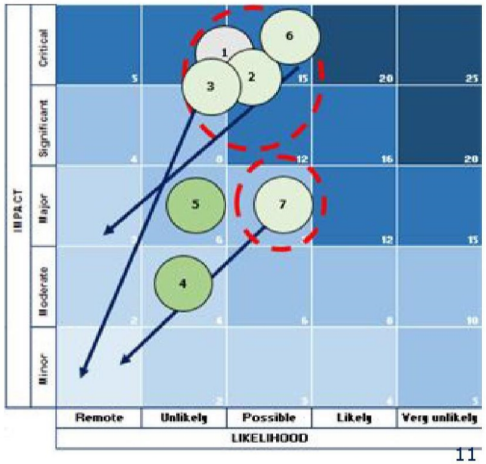
- **Regulatory obligations:** Averse
- **Non-Regulatory obligations:** Minimalist
- **Employment:** Cautious
- **Litigation:** Minimalist
- **Fraud & Theft:** Averse

The appetites have been identified using a 5 point (draft) Appetite scale provided as an Appendix.

A supporting Dashboard is being developed which links the (then) current ratings of individual risks, the KRI trends and how these relate to the associated risk appetite. This consolidated analysis will inform the action (if any) that should be taken in the next reporting period to manage the risks.

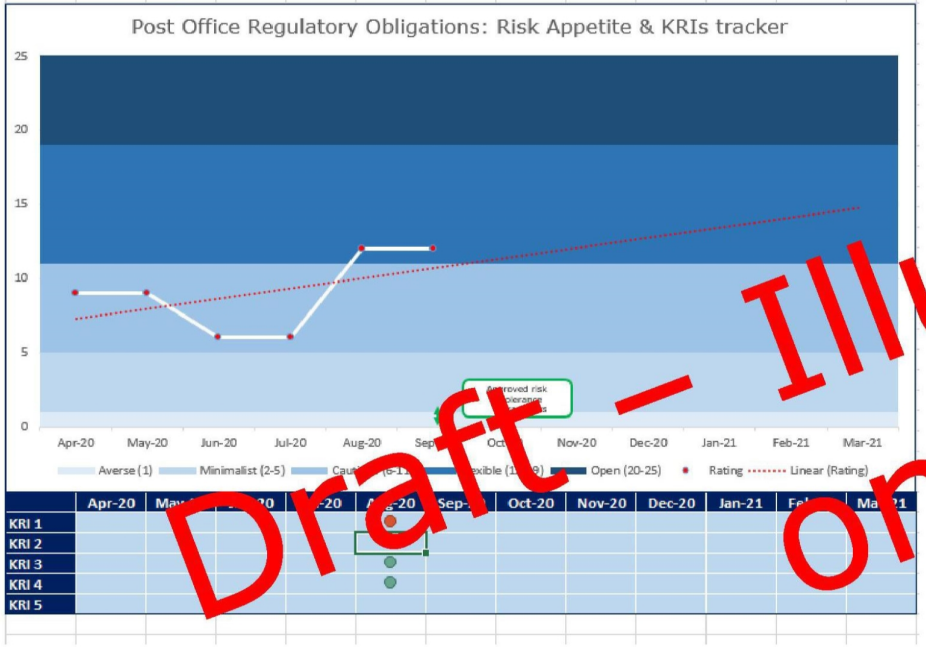
An illustrative Dashboard along with a typical action plan is provided in the following slides.

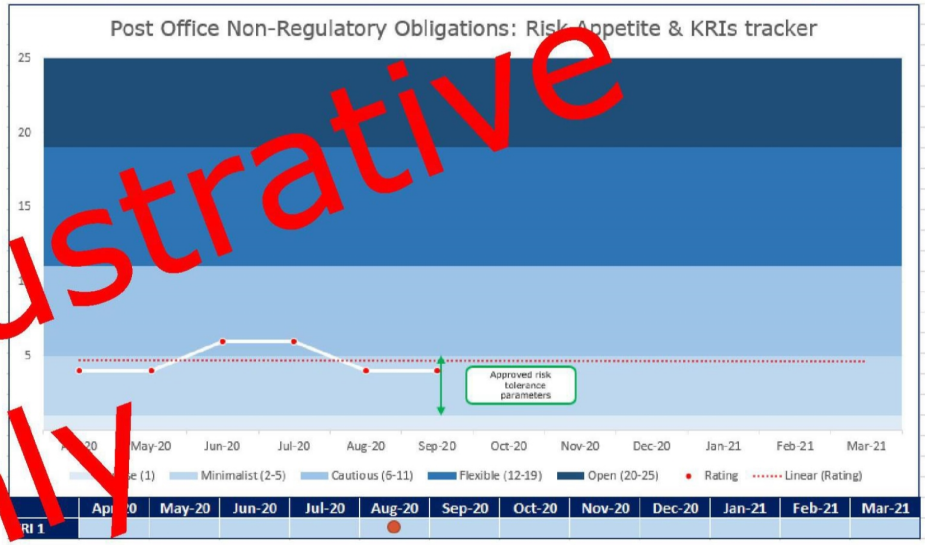




POL00401629

(i) Regulatory (ii) Non-Regulatory Obligations





Draft – Illustrative only

Analysis & Next Steps

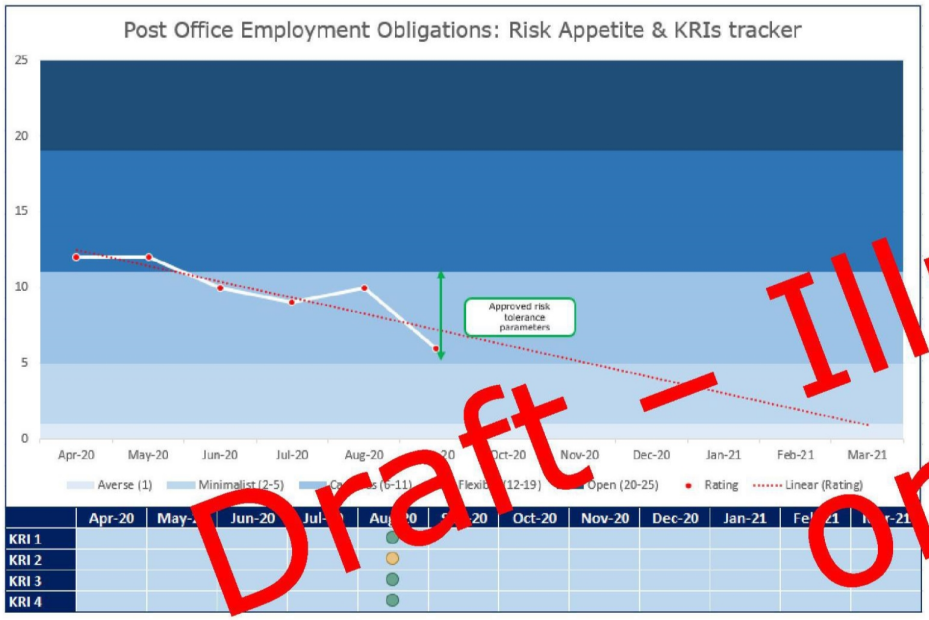
3 risks outside appetite with worsening trend. Although 3KRIs report within tolerance, 1 is breaching. Urgent work required to resolve anomaly either through reviewing current impact and likelihood scores of risks and/or tightening KRI tolerances.

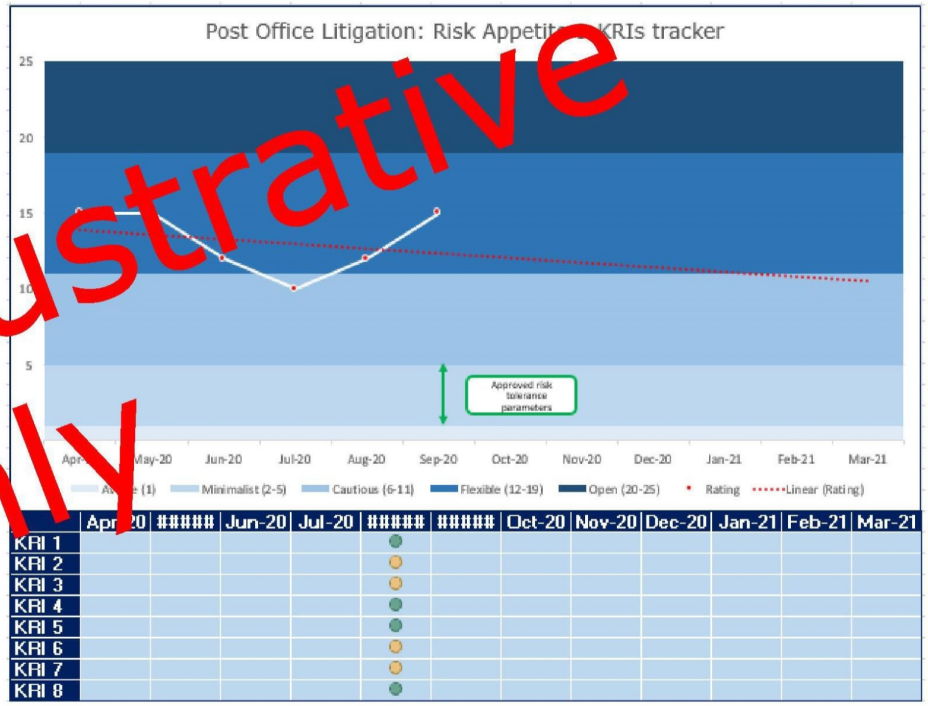
Analysis & Next Steps

Risk within appetite with stable trend but KRI has just breached tolerance. At this stage risk current impact and likelihood score is satisfactory. KRI should be monitored to determine trend. No further mitigations required at this point. Risk should continue to be tolerated.

POL00401629

(iii) Employment Obligations (iv) Litigation





Draft – Illustrative only

Analysis & Next Steps

Risks within appetite with improving trend. KRIs broadly acceptable although 1 has recently breached tolerance. Must be closely monitored to ascertain whether this is a sign of worsening position.

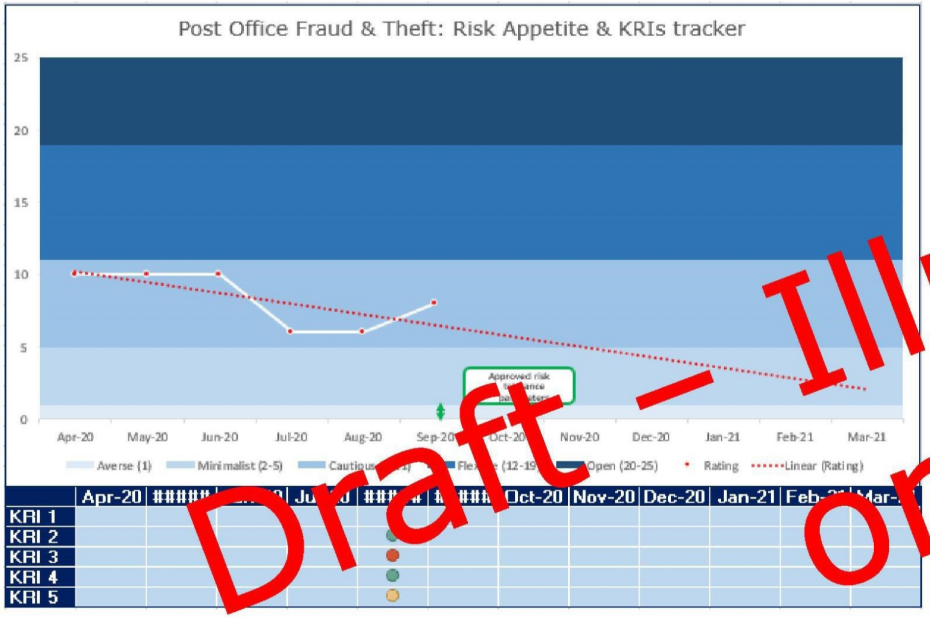
Analysis & Next Steps

Risk is significantly outside appetite and trend is worsening. 4 of the 8 KRIs have breached tolerance. Work of the highest priority required to reduce risk current impact and likelihood scores – current trend forecasts this will not happen until 3/2021

Strictly Confidential

POL00401629

(v) Fraud & Theft



Draft – Illustrative only

Analysis & Next Steps

Risk outside of appetite and trend has slightly worsened. 1 KRI is rated RED and another Amber. Work required to reviewing current impact and likelihood scores of risks and/or associated mitigations

Strictly Confidential

POL00401629

Appendix: Post Office Risk Appetite scale

Appetite rating	Risk taking philosophy	Tolerance for Uncertainty[1]	Decision choice[2]	Prioritisation of Strategic Objectives[3]
Open	Will take justified risks and accept the possibility of failure	Will accept the possibility of failure	Will choose the option with the highest return	Will accept risks could materialise and the achievement of (some) strategic objectives could be compromised
Flexible	Will take strongly justified risks	Will choose the option which has some degree of risk	Will accept risks subject to being able to proactively manage its adverse impact	Will accept (under certain conditions) the achievement of (some) strategic objectives could be compromised
Cautious	Prefers safe delivery to risk	Will accept a limited circumstances risk could materialise	Will accept risks could materialise but only if their adverse impact are limited and are heavily outweighed by benefits	Would prefer ideally not to accept risks materialising if this meant the achievement of (some) strategic objectives could be compromised
Minimalist	Will only take an extremely conservative approach to risks	Will accept risks could materialise	Will accept but only if activity is essential and the possibility and extent of failure is limited	Would be extremely reluctant to accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised
Averse	Will avoid risks where at all possible	Has an extremely low appetite for risks to materialise	Will always select the option with the lowest risk.	Will never accept risks materialising if this meant the achievement of (some) strategic objectives would be compromised

Draft – Illustrative only

[1] **Tolerance for uncertainty:** How willing is the Post Office to accept uncertain outcomes? This illustrates the Board's appetite to trade off certainty to achieve a given objective. A low rating demonstrates the Board's need for certain outcomes, while a high rating shows the Board will pursue an objective even with an uncertain outcome.
[2] **Decision choice**: When faced with multiple decision options, how is the Post Office willing to select a decision that puts a strategic objective at risk? This question assesses the Board's acceptance that a given choice may lead to failure to meet a strategic objective. A Board who are averse will only choose options that pose a minimal threat to the strategic objective's achievement. A Board open to this risk are willing to trade off the possibility of failure for a high-risk, high-reward decision.
[3] **Prioritisation of strategic objective**: How willing is the Post Office willing to trade off this specific objective against achievement of other objectives? This demonstrates the Board's willingness to pursue achievement of a given strategic objective over achievement of another. A Board who are averse to this would never trade off completing the objective in question for failure of other objectives. A Board which is open would be willing to accept this trade-off.

Strictly Confidential

POL00401629

3

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Risk, Compliance and Audit Report	**Meeting Date:**	10 September 2020
Author:	Mark Baldock: Head of Risk Jonathan Hill: Director, Compliance Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer Ben Foat: General Counsel

Input Sought: Noting

Previous Governance Oversight: Not applicable

Executive Summary

This paper provides an update on key and emerging risks, compliance matters and an update on the latest internal audit position. The Committee is asked to:

1. Note the Risk update, which is presented in the attached Central Risk Dashboard, in particular:
   - Summaries of key enterprise, intermediate, local and change risks; and
   - Draft risk appetite statements and key risk indicators (KRIs) for illustration purposes.

2. Note the Compliance update, in particular:
   - The on-going focus by Ofcom on the Telecoms industry;
   - The growth in GLO/Historical Shortfall Scheme related FOI requests and DSAR;
   - The continuing growth in SARs and investigations being managed by the Financial Crime Team; and
   - The activity being undertaken to manage the AML and Safety risks arising from the significant growth in cash deposits by Money Service Businesses in branches.

3. Note the Internal Audit update, in particular:
   - Progress being made with delivery of the Internal Audit programme; and
   - Status of internal audit actions.

Confidential

POL00401629

3

Compliance

Telecoms

Telecoms Providers' response to Coronavirus

1 Given our strong call centre performance during the pandemic and that Ofcom have resumed normal duties, Ofcom has agreed to our request to stop the fortnightly reporting. We have agreed with Ofcom to extend our commitments in line with the major operators and have also agreed with the NHS that we will run our offer until September. DCMS has also reached out to us and asked us to commit to not having any broadband usage caps.

Fairness

2 In early August, Ofcom wrote to Nick Read requesting a meeting in September/October to discuss Post Office performance against the Fairness Commitments. Ahead of this meeting it has asked Post Office to supply information on the progress we have made since signing up to the commitments, as well information on our plans for the year ahead. Work is underway preparing the response.

3 At our last meeting with Ofcom it said that it considers customers as "vulnerable" when they have been out of contract for a long time e.g., 2-3 years. Ofcom thought Post Office would be near the top of providers with a high percentage of out of contract customers (paying higher prices than in contract customers) and wanted to see progress on this. The introduction of Annual Best Tariffs will go some way to address this (see below). However, given timings of the RFP and budget constraints Post Office has not been able to go beyond the regulation.

Annual Best Tariff Notifications

4 Following on from the introduction of End of Contract Notifications, Post Office is required to send Annual Best Tariff Notifications (ABT) to customers who have been out of contract for more than a year and not received an End of Contract Notification. The ABT must be sent by 14th February 2021. The first ABTs are due to start going out at the end of October and will be done in a phased approach. It is expected to drive more calls to the contact centre and drive complaints as people will query why their current price is higher than the new offers in their communications.

Voice only customers

5 The Telecoms Team is reviewing the impact of Project Galaxy on its customers. Galaxy was Post Office's response to Ofcom's 2017 intervention in the voice only market, which saw BT reach a voluntary commitment with Ofcom to reduce its pricing by £5. Ofcom has been requesting information to help it understand the impact the voluntary price cap has had on the market and customer engagement. It is not clear at this stage what action they will take.

6 Through Galaxy, customers who had a vulnerability flag on their account were automatically moved to the cheaper voice only plan but could take the combined broadband and voice offer. All other customers were automatically opted into the combined broadband and voice plan but could opt out and take the cheaper voice only plan. Not all customers that were opted into the combined plan requested the router, which is necessary for them to take advantage of Post Office broadband. Compliance has recommended that action needs to be taken with these customers.

7 The Telecoms Team is reviewing its options and as a first initiative is planning on issuing a reminder to customers on their bills to request a router, which can be done relatively quickly.

Confidential

POL00401629

8 Post Office has planned a price change for September that will impact voice only customers. A risk has been raised that following the price change, Post Office may be forced to reduce our prices back down, possibly even lower than the original price, as Ofcom review of the market could, in a worst case scenario, introduce retail regulation.

PSD2

9 Following confirmation from the FCA on our approach, work is underway to submit a first ECE Notification and prepare for a regulatory audit in 2021. We are going through the procurement process to select the auditor in order to meet this obligation.

European Electronic Communications Code

10 The new European Electronic Communications Code (EECC) will impose new regulatory obligations on all providers. These obligations will include changes to the switching process, additional information about contracts, provision of pre-contract information and accessibility obligations.

11 We are waiting for Ofcom's consultation in September where they will outline how they plan to implement the EECC. Ofcom has confirmed providers will have 12 months following the consultation to implement the changes

Data Protection

GLO and Historic Shortfall Scheme

12 Compliance has been working with the GLO project to identify, locate and provide all data required to support the various ongoing initiatives, in particular;

- Working with the Historic Shortfall Scheme to manage and answer all requests for information and data to support applications, this work is complex and likely to run into Q4. As at 26th August 2020, there are currently 174 live requests, this number may rise as a result of the upcoming Stamps scheme.
- Provide information to support those cases that have been referred by the CCRC. These searches are complex, and Compliance is working with external law firms to identify, locate and extrapolate all information that may be required by the Court

13 In addition, there has been a significant rise in complex Freedom of Information Requests relating to GLO matters which are being managed with support from external Counsel.

14 We have received 40 FOI requests from one individual that has been actively blogging and reporting throughout the GLO process. Working with external Counsel these requests will be rejected on the grounds that they are Vexatious (Section 14 FOI Act).

15 In response to specific requests for information the team have identified 31k boxes of files currently with Oasis contain hardcopy documents returned by branches that are closed. We do not know exactly what documents are inside these boxes as there are no external indexing outside the boxes.

16 They are likely to contain branch balancing data, trading statements, daily and weekly reports. They may also contain HR files such as P250 assistant verification and contractual information on the agent/postmaster

17 Meetings are ongoing with internal legal, Peters and Peters, HSF to determine the significance of this information on the CCRC and HSS projects. set

AWS Move to the Cloud:

18 IT Strategy is to exit the Belfast Data Centre in 2021 and move Horizon to a cloud-based solution. Due to the size, scale and complexity of this move an aggressive timescale has been

POL00401629

19 Fundamental to the transition is the management of the risk to the integrity of Horizon data and the implication for Post Office upstream clients such as Government, Banking Services and Bill Payments contracts. Government, Royal Mail and the Bill Payments/Payout clients have been contacted. Legal, Compliance and IT are currently working through questions to Post Offices IT proposal, it is anticipated that a high level of acceptance will be achieved

20 Notification to the Banking Framework group is planned for w/c 01st September in line with IRRELEVANT

21 A tactical decision been taken by the CIO and their team to do what is necessary in order to allow the AWS migration from Belfast to take place, without any added 'future proofing' to make other subsequent cloud implementations easier.

Implications of Schrems II case and Privacy Shield:

22 A case was brought before the CJEU challenging the use of Privacy Shield for International Transfers of Personal Data from the EU to the US.

23 The CJEU recently found in favour of Schrems stating that organisations could no longer rely on the use of Privacy Shield to legitimise transfers to the US. The exposure to Post Office to this part of the ruling is minimal and will cause no significant issues.

24 The CJEU went further in its findings casting doubt over the validity and use of Standard Contractual Clauses (SCCs) to legitimise transfers not only to the US but to anywhere outside of the EU.

25 The European Data Protection Board will be producing new SCCs considering this ruling. If Schrems is successful in his challenge to the SCCs, or significant changes are introduced, then this will have a significant impact on Post Office contracts where personal data is stored outside of the EEA.

26 The extent of Post Office exposure is being considered with a report being produced for future RCC meetings.

GDPR Contract Remediation;

27 The Contract Remediation project was formally closed at the end of July as reported to the previous RCC. Work is ongoing on the 8 outstanding contracts which, due to their complexity, are likely to continue for some time.

28 Monthly CRG meetings continue to monitor progress and support negotiations. This will continue until all outstanding contracts are finalised.

Financial Crime

Compliance with Money Laundering Regulations

29 Between 20th June and 19th August, 153 Bureau de Change cases were identified, up 53% on the same period 2019. There has been an increase in branches splitting transactions and customers visiting multiple locations, although some of these are genuine and linked to low stock levels in branch in June/July. Some branches have split transactions to amounts under the ID threshold following the initial amount failing eKYC. These have been escalated to the relevant area and contract managers to remedy.

30 The data fix for Sanction screening has been implemented and two potential Sanction declines were reported in early August, although on review, neither were exact matches. The customer data for these transactions was present in AML Credence. However, not all transaction information flowed through. This has been escalated to DCoE, which is investigating with Accenture.

31 Suspicious Activity Reports ("SARs") and investigations have reached record levels since March, with 1,063 SARs and 191 investigations in June & July (767 and 109 in June & July

POL00401629

2019). SARs for July 2020 reached the highest level seen since 2015, when records started. Of those received from the Network and CViT, the majority relate to MoneyGram and high value banking cash deposits.

32 Due to increased workloads, approval has been obtained for an additional Fixed Term Contract PO grade in Chesterfield until the end of March 2021. If volumes continue at current levels, this will need to be a permanent role for 2021/22.

33 Post Office has been advised that we have been assigned a new HMRC regulatory supervisor, as the individual who took over when Lee Simpson retired in May has moved to a new role. An introductory meeting is scheduled for 30th September.

34 A further meeting was held with HMRC on the forthcoming fees consultation. It has considered the options and points we have previously raised and advised that some suggestions relating to turnover and tiered approaches will be in the fee consultation. There are currently no agreed timescales for when this will be published.

35 In response to the 2019 Government's Economic Crime plan, HMT has published a consultation on an Economic Crime Levy, which it plans to introduce for the AML-regulated sector to fund measures to combat economic crime and money laundering. The consultation is currently being reviewed by Legal and Compliance and responses are required by 13th October 2020. There is a risk that this could increase Post Office costs by over £1m per annum.

36 Financial crime risk assessments have been hampered by lack of engagement by some product managers. Compliance re-scheduled assessments to support business critical priorities during the Covid lockdown, but recently the MLRO has had to send chasers via some Product Directors.

37 To address these issues, activity is planned during Q3 to raise awareness with Commercial teams about their responsibilities under Post Office policies and the importance and benefits of these risk assessments. Updated content is planned for the Financial Crime intranet page to aid Product Information Pack and post-assessment action plan completion.

38 Compliance approved a trial to remove in-branch ID verification for online Drop & Go applications at the start of Covid. The product team also included in-branch applications, although this was not part of the proposal approved by Compliance. Data has been reviewed and shows that the pilot has been commercially successful, and there have been no issues to date. We have approved this as a permanent change, subject to the risks being called out on the Commercial team's RACM and that action is taken to address and remove duplicate accounts.

Anti-Bribery and Corruption ("ABC") update

39 The IT issues relating to the new gifts and hospitality tool have now been resolved. Reporting has remained low during lockdown.

40 Annual ABC training is due to be launched 5th September, and a number of communications and reminders are planned during August and September.

Whistleblowing Update

41 There has been an increase in new reports during Q2 2020/21, with 8 reports received compared to 4 in the same period last year. Most relate to reports from agent assistants about activity in branches.

POL00401629

42 The two cases which were previously on hold due to Covid-19 are now being investigated by Area Managers and should be concluded in September. There have been no other impacts caused by Covid-19 or working from home, and there have been no changes to the report types and categories received.

Fit & Proper update

43 The agent F&P data solution went live in July, and the first cohort of 500 agents was put through the re-declaration process, with all agents responding by the due date. The second cohort commenced 17th August and includes all Commercial Partners.

44 Circa 1K temporarily 'paused' branches have been re-instated, and HMRC has agreed that the premises fees for these will be deferred to 1st December in line with our annual registration fees.

45 The monthly agent data for July was c.1 week late due to issues manually appending agent data as the change request to annotate the 'paused' branches in the new system has not yet been delivered. HMRC were contacted and approved the delay. The next monthly data is due 28th August and will be delivered on time.

46 A previously identified issue relating to registration and missing agent data for branches in a 'Short Term Temporary Closed' status for extended periods (in some cases over 18 months) is being investigated by the Network Development Team to ensure that a policy and process is in place to manage branches in this status and where there is no longer a postmaster contracted to run the branch.

47 A new flag has been added as a mandatory field in Success Factors for all job requisition approvals which will drive weekly reporting to ensure that all employees in relevant Post Office roles undertake the HMRC F&P test, and that when individuals move to different roles/leave Post Office, they are removed from the HMRC register.

External Threats

48 We continue to support the Covid Fusion Cell, and the sub-group looking at cash-based money laundering. Criminals continue to exploit COVID-19 and concerns remain about the effect that the downturn on the economy will have on the recruitment of mules to launder the proceeds of crime. Compliance has continued to deliver branch communications on scams and COVID-19 related fraud.

49 There continues to be concern about high value banking cash deposits relating to Money Service Businesses in East London, and liaison with the National Economic Crime Agency is ongoing. We are working with the Supply Chain, Network, Security and Banking teams to address the AML and people safety risks. A workshop to find solutions that remediate these risks is being held w/c 7th September. In order to continue to accept these deposits it is essential that these risks are addressed.

50 We have been advised by an HMRC investigator that information we provided concerning high value cash deposits being made early on in the Covid lockdown at a branch in Manchester, has led to a £78K seizure and multiple arrests.

Supply Chain Compliance

51 The Health & Safety team approved travel and on-site compliance assurance work from July – a risk assessment is completed ahead of all compliance assurance activity. 3 compliance assurance visits have been completed including Note Circulation Scheme (Bank of England) at Midway House and Bristol & Swansea ahead of the external audit scheduled for September.

52 Additionally, a trial remote compliance assurance of the licence management team was completed – learnings from this will be used to enhance future assurance activity and reduce time spent on site.

Confidential

POL00401629

53 7 improvement needs were raised in total with no significant issues identified.

54 Following request by the product team, a review of VOW stock discrepancies was completed and learnings shared with Supply Chain and the Head of Loss Prevention. Whilst Post Office is terminating the relationship with VOW, the findings highlight areas where stock control can be improved generally.

55 Compliance identified an issue relating to value stock pouches that were not showing as delivered in stock systems, and the findings have been shared with Supply Chain and the Head of Loss Prevention. System, reporting and management controls are currently being reviewed and enhanced by Supply Chain.

Financial Services

Compliance Monitoring

56 Compliance is currently supporting the business with support and communications on preparing for business re-invigoration in the post lockdown environment.

57 The key resumption of activity will be Travel Insurance (TI) sold in branch on September 14th. The branch-based policy has not been sold since March and it is significantly different from that previous version sold with 3 layers of cover and new Covid 19 conditions that will need to be disclosed clearly at point of sale.

58 The interim training solution produced by POI (Microsoft Sway) relies on Postmasters using personal devices to access an online training and test. Compliance has supported the training solution provided that

- It is clear that only the individual that has taken and passed the training is the individual that gets given access to TI sales on Horizon. This is consistent with our Smart ID Principles for regulated sales including mails, savings, telecoms and other insurance sales.
- The L&D team support the changes to Horizon and training systems

59 From August a small number of mystery shops for POI protection business has resumed, a wider mystery shopping (BoI, Telecoms, Insurance) will resume in Q3, including for the re-launched travel insurance business.

60 As Lead Principal POI are leading a Multi Principal review of PO 1st Line Oversight and Controls. The scope of the review is wide ranging covering, internal governance, risk management framework, training, AR responsibilities, quality of sales oversight and roles and responsibilities. This will involve the compliance teams of POI, BOI and Capital One.

61 The compliance team will support the provision of materials for the review and assist the fieldwork a draft report is expected before the end of 2021.

62 FS Regulatory updates

63 A summary slide of the key future developments is included in the reading room, a number of planned changes have been delayed whilst the regulator focuses on managing the crisis.

64 On Access to Cash the FCA made a surprise draft guidance announcement in July (ahead of any potential Government legislation on this issue) that all Banks planning to reduce their branch Network or close ATMs had to report their plans to them including how they will ensure access to cash is maintained. This demonstrates the regulatory concern related to 'access to cash' and the cost pressures Banks are under to try and slim down their Networks. The Post Office Banking Framework is a key alternative for these customers.

65 The FCA provided the second part of its Vulnerable Customer guidance consultation in July. The guidance focusses on:

- understanding vulnerable customer needs,
- front line individual skills and capability,

POL00401629

- product design and provision,
- customer communications and
- monitoring of performance

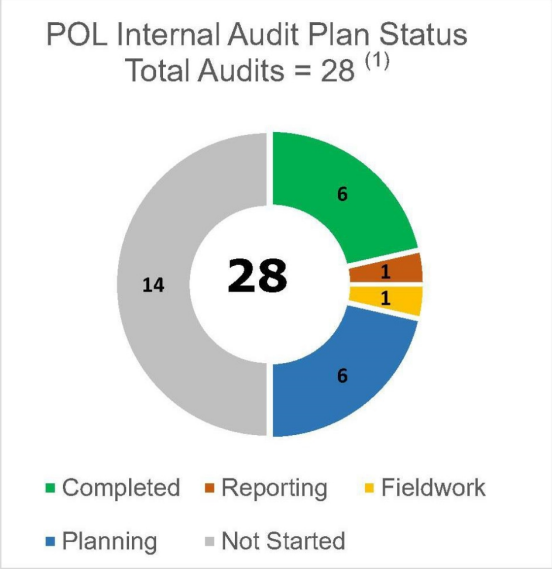
66 We do have a number of measures in place to support vulnerable customers but there is always room for improvement. We will work with our Principals on any areas identified and more generally through the Vulnerable Customer Action Group.

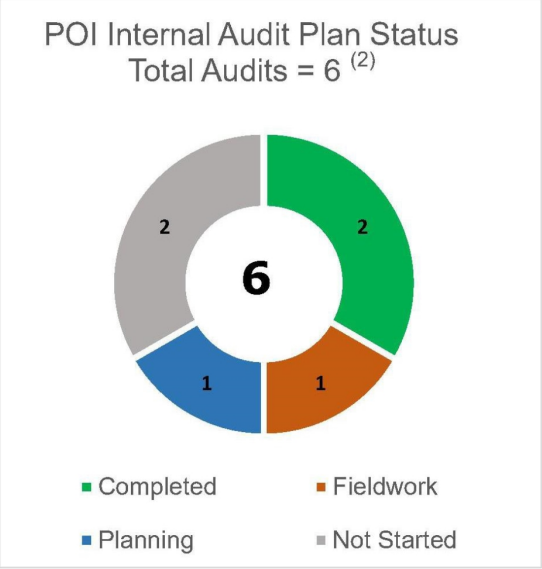
Internal Audit

Progress with Internal Audit plan

67 Delivery of the 2020/21 programme is making good progress, having completed seven reviews since the July ARC meeting (5 POL & 2 POI). This includes an interim report on our current review of the Belfast Exit programme.

68 Current delivery status is as follows:





(1)Target number of reviews based on revised plan for 2020/21 (to be approved by ARC) (18 Internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 5).

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

69 A re-prioritised Internal Audit programme was approved at the May ARC meeting in response to Covid-19. It was agreed that a more dynamic (quarterly rolling) audit plan will be adopted and reviewed at each ARC. The latest re-prioritised plan is included in the reading room (Appendix 5).

Confidential

POL00401629

70 The following audits are being planned for delivery in Q3:

	Review	Sponsor	Timing	Status
1	Effectiveness of Second Line during COVID-19	Al Cameron / Ben Foat / Jeff Smyth	Ph1-June Ph2-Aug	Complete Reporting
2	Historic Matters (Post GLO) Set-up and Governance	Declan Salter	Oct	Planning
3	Historic Matters (Post GLO) Operations Improvement Programme (Common Issues Judgement)	Julie Thomas	Nov	Planning
4	Mails & Parcels	Owen Woodley	Oct	Planning
5	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Oct	Not started
6	IT Controls Framework (Phase 1 – Gap Analysis)	Jeff Smyth	Sept	Planning
7	Controls over Revenue Adjustments	Al Cameron	Sept	Fieldwork
8	Identity and Access Management (JML) – Gap Analysis	Jeff Smyth	Sept	Planning
9	Branch Hub (Programme Assurance)	Julie Thomas	Sept	Planning
10	Belfast Exit (Programme Assurance) Phase 2	Jeff Smyth	Oct	Planning

Internal Audit reviews completed

71 The following five POL audits were completed since the July ARC meeting:

1	GLO Historical Shortfall Scheme - Data Validation	
2	Maintain Minimum Control Standards during Covid-19	
3	RMPP (DB Pension Scheme) - Data Errors (Final Draft Report)	
4	Health & Safety Response to Covid-19 (Final Draft Report)	
5	Belfast Exit Programme Assurance – Phase 1 - Interim Report	

72 Our findings and observations from these reports are summarised below, with the full reports available in the reading room (appendices 6-10).

[redacted]

Confidential

POL00401629

2. **Minimum Control Standards during Covid-19** (Ref.2020/21-05)



Needs Improvement

Sponsor:
Al Cameron / Ben Foat / Jeff Smyth

Audit actions:

P1	1
P2	5
P3	1
Total	7

Appendix 7

The purpose of this audit was to consider the impact to key controls from changes in processes as a result of operational challenges arising from Covid-19, and to ensure that minimum control standards are operating effectively.

This report consolidates the findings from the three interim reports previously issued, i.e. Cash Controls (Phase 1), Financial Reporting Controls (Phase 2) & IT Controls (Phase 3).

We conclude that during its response to Covid-19, Post Office maintained a strong control environment in its key business areas, with minimal reduction in controls. Where, of necessity, there have been control adjustments, these were recorded and signed off as appropriate.

However, we noted some areas for improvement, most notably the maintenance of audit trail and evidence of control operation (which was impacted by remote working), as well as a need to update documentation to reflect the actual controls in operation.

Management Comment

Finance and Ops:
"It is pleasing to see that despite the challenging situation a strong controls environment was maintained with adjustments made in a timely, thoughtful and efficient manner. We note the minor findings identified and these have already been addressed via updating of relevant documentation."
Kathryn Sherratt – Finance Director (for Al Cameron – Group CFO)

IT:
" This report is an accurate and fair reflection of the challenges and tensions we have had to manage to keep the entire organisation working through a challenging time during key absence and also against a backdrop of the Pandemic. We note the findings and have added those into our wider IT controls piece being led by Tony Jowett and Aatish Shah."
Tony Jowett – CISO/Interim IT Director (for Jeff Smyth – Group CIO)

3. IRRELEVANT **(Final Draft Report)** (Ref. 2020/21-09)

Not Rated
(Lessons Learned Review)

Sponsor:
Al Cameron / Lisa Cherry

Audit actions:

P1	1
P2	4
P3	1
Total	6

Appendix 8

IRRELEVANT

Management Comment

tbc

Confidential

POL00401629

4. **Health & Safety Response to Covid-19** (Ref. 2020/21-04)	
 Needs Improvement ***Sponsor:*** *Al Cameron* Audit actions: P1: 1 P2: 6 P3: 0 Total: 7 *Appendix 9*	The objective of this audit was to provide assurance that the Health and Safety response to Covid-19 has provided the necessary protection to postmasters, colleagues and customers, and that adequate safeguards are in place to permit a return to PO admin centres in a Covid secure way as and when required. Health & Safety have been critical in driving an effective response to Covid-19. They were instrumental in the sourcing and provision of PPE to the branch network and Supply Chain and the risk assessment of PO's responses to the crisis throughout. Whilst ensuring the continued safety of postmasters, colleagues and customers they have also been heavily committed to providing responses to urgent requests for information from key stakeholders. However, the audit also highlighted some areas needing improvement, most notably completion of risk assessments and the lack of accurate and timely management information.
Management Comment **tbc**	

5. **Belfast Exit – Follow-up (Phase 1 Set-up & Governance)** (Ref.2020/21-11)	
Not Rated (Interim Report) ***Sponsor:*** *Al Cameron* Management comments and audit actions will be in the final report at the end of phase 2. *Appendix 10*	The Belfast Exit Programme has the objective of migrating the services running in the Belfast datacentres to the Cloud. This mitigates the end-of-service-life risk and cost associated with the hardware residing at the datacentre and the supporting Oracle Database. The estimated total project spend is circa of £32m with full benefits being re-assessed (a £4m benefit is expected in FY21/22). Internal Audit is performing a follow-up review of the programme, to provide assurance that the revised programme set-up, governance and delivery processes are fit for purpose and operating effectively to enable the envisioned benefits of migrating to the cloud. Phase 1 of the review focussed on the revised programme set-up, team and approach. In our view the approach being followed is sound and programme set-up should enable the delivery of the agreed benefits, although we highlight that timelines are compressed with no contingency. The programme is in fact two mutually dependent sets of activities with some conflicting priorities - the fast migration and decommission of applications and data; and the setup of a Post Office Cloud Centre of Excellence (Cloud Office) that benefits from an optimised BAU, with balance between each needing to be carefully managed. Audit actions raised in the previous Belfast Exit audit are currently being addressed, the majority of which are deliverables to be done following the Migration Readiness Phase (MRP), planned to be completed in October.

Post Office Insurance (POI) Audit Programme

73 The table below shows the status of the POI audit programme:

	Review	Timing	Status
1	Cyber Security (POL-POI Gap Analysis)	Aug	Reporting (Sept ARC)
2	Incident and Breach Management	Aug	Reporting (Sept ARC)
3	Data Governance: ethics, security and privacy	Sept	Fieldwork (Nov ARC)

Confidential

POL00401629

4	Effectiveness of Risk Management – original plan	Q4	Not started
5	Channel review: Non-branch sales – original plan	Q4	Not started
6	Pricing: Principles, policies and process	Nov	Planning

Status of Audit Actions

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

75 The movement and ageing of audit actions are shown in the table below (status at 03 September 2020).

Audit Action Status (POL):	
Open actions at last ARC	48
Less: Actions closed in period	14
Add: New actions in period	12
Total open actions	**46**

Ageing:	
Open (not yet due)	43
Overdue (<60 days)	3
Overdue (>60 days)	0
Total open actions	**46**

76 Following is a summary of the 3 overdue actions and latest status update:

Description of audit finding and Priority rating	**GE owner and due date**	**Action Owners and Status Update**
Data Privacy		
Legitimate Interest Assessments (LIAs) have not been undertaken in all instances where legitimate interest has been selected as the basis for data processing. **(P2)** **Action:** The DP team will work with the business to ensure that outstanding LIAs are completed.	Ben Foat 31/08/2020	**Owner:** Chris Russell Completion of action delayed by a major incident that had to take preference. The action is expected to be completed before the ARC meeting.
Telco Billing		
Operation of all corrective controls, implemented after the PwC review, has not been sustained **(P2)** **Action:** 2(a) Review actions taken as a result of the PwC investigation (and reported to the ARC) to confirm new controls are in operation or issues have been fully resolved. **Action:** 2(b) Re-clarify and re-document roles and responsibilities of Telco teams (finance and commercial functions) and Central Finance to ensure all processes and controls over financial reporting operate as intended.	Owen Woodley 31/07/2019	**Owner:** Kathryn Sherratt & Meredith Sharples Progress wasn't satisfactory and / or insufficient evidence to close the actions. This was escalated to GE and is now being addressed with a target completion date before the ARC.

Confidential

POL00401629

3

Reading Room Appendices[1]

Compliance

Appendix 1: Compliance Dashboard (Summary)
Appendix 2: Compliance Dashboard
Appendix 3: FS Regulatory Calendar
Appendix 4: Telecoms Regulatory Calendar

Internal Audit

Appendix 5: Internal Audit Plan for 2020/21
Appendix 6: Internal Audit Report – Historical Shortfall Scheme – Data Validation
Appendix 7: Internal Audit Report – Minimum Control Standards during Covid-19
Appendix 8: Internal Audit Report – IRRELEVANT
Appendix 9: Internal Audit Report – Health & Safety Response to Covid-19
Appendix 10: Internal Audit Report – Belfast Exit – Interim Report

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

Confidential

POL00401629

POST OFFICE LIMITED
RCC Paper

4

Title:	Project Assurance – RM Pensions (POL Section)	**Meeting Date:**	RCC 10.09.2020
Author(s):	David Scothern Maxine Cross Laurence ONeill	**Sponsor(s):**	Al Cameron Lisa Cherry

Input Sought:

Noting that:

- work remains in progress to IRRELEVANT
- IRRELEVANT
- an internal audit, commissioned to examine related processes/systems, is reporting back at this meeting

Decision:

IRRELEVANT

and IRRELEVANT That was also the decision of the last ARC. Since the last ARC, however, several new facts have arisen which are described in the section IRRELEVANT below. In view of those new facts, and having regard to POL's risk appetite, whilst it remains the case that IRRELEVANT it is recommended that a IRRELEVANT Given the timing ARC would need to be notified of this IRRELEVANT Does RCC support this recommendation?

Previous Governance Oversight

CR approved 11.8.2020 in relation to the IRRELEVANT

IRRELEVANT

ARC paper 27.07.2020 to notify ARC of the IRRELEVANT advise ARC of the approach being taken IRRELEVANT and seek support for the recommendation that it was IRRELEVANT IRRELEVANT

Executive Summary

In July ARC was advised of IRRELEVANT IRRELEVANT These are set out by way of a reminder in this paper. ARC was asked the question

IRRELEVANT

An internal audit report, commissioned to identify IRRELEVANT IRRELEVANT and to ensure lessons are learnt concluded:

Confidential

POL00401629

IRRELEVANT

The work to IRRELEVANT IRRELEVANT IRRELEVANT Independent verification of this work has started. Once the work and the verification are complete the next steps are to:

4

- IRRELEVANT

Work is also continuing to ensure communications plans of POL and the Trustee remain aligned:

- Annual Benefit Statements (ABS) for IRRELEVANT IRRELEVANT
- Meetings have taken place with the Unions on 19 August 2020 and again on 1 September 2020. We are seeking to ensure our plans are aligned although IRRELEVANT The Unions also wish to be involved in decisions about IRRELEVANT IRRELEVANT
- The Press Office has reactive lines in place to deal with any interest from the press in the event of whistleblowing or press reporting following the IRRELEVANT IRRELEVANT

Questions addressed

1. By way of a reminder IRRELEVANT
2. By way of a reminder, IRRELEVANT IRRELEVANT
3. By way of a reminder, are the likely impacts on the a IRRELEVANT IRRELEVANT
4. By way of a reminder, what are the legal risks from the IRRELEVANT
5. What are the Stakeholder implications?
6. Has the position about IRRELEVANT changed?

Report

IRRELEVANT

An internal audit by Deloitte was commissioned with objectives as follows:

POL00401629

- Conduct a lessons-learned exercise, to identify the background and causes of the issues observed.
- IRRELEVANT
- Review the future processes designed by Post Office Limited and assess the robustness of their design.

4

The findings were

- IRRELEVANT

Overall Deloitte was satisfied with the robustness of the future processes and made the following observations:

IRRELEVANT

The full report is included in appendix 1

Are there any changes to the IRRELEVANT

No IRRELEVANT remain as reported to ARC on 27 July 2020.

Financial Impact

IRRELEVANT

Confidential

TAX-#30312822-v1

POL00401629

IRRELEVANT

4

Risk Assessment, Mitigations & Legal Risks

Risk	Considerations/Mitigations	RAG
IRRELEVANT		
IRRELEVANT	[redacted]	

Confidential

TAX-#30312822-v1

POL00401629

4

IRRELEVANT

Has the position about IRRELEVANT **changed?**

[redacted]

5

Confidential

TAX-#30312822-v1

POL00401629

[redacted]

4

How does IRRELEVANT change the communications timeline?

The key communication milestones are set out below:

- 28th September: IRRELEVANT receive Annual Benefit Statements
- 21st September: IRRELEVANT IRRELEVANT
- 15th September: Meeting with Unions to co-ordinate communications
- 10th September: Recommendation to IRRELEVANT

The Unions' approach is to IRRELEVANT IRRELEVANT At the meeting on 15th we expect to have to set out the principles underpinning our approach for inclusion in those communications, which could lay bare the differences between the two sides. In preparation for that meeting it is recommended we have a letter to employees ready for sending out.

Other Options Considered

IRRELEVANT

Actions Taken Since the Last Report

IRRELEVANT

- Two meetings with Unions with aim of ensuring alignment of the respective communications

IRRELEVANT

Next Steps & Timelines

IRRELEVANT has produced a narrative based plan (see draft at Appendix 3) and is developing the timescales for each of the stages outlined. Beyond the immediate activities, the timescales shown below are indicative

Confidential

TAX-#30312822-v1

POL00401629

- September
  - If instructed to do so by RCC, IRRELEVANT
  - IRRELEVANT
  -
- September- October
  -
  -
  -
  -
- October onwards
  -
  -
  -
  -
  -
  -

4

IRRELEVANT

IRRELEVANT

Confidential

TAX-#30312822-v1

POL00401629

Appendix 1

- See Deloitte's Internal Audit Report - part of Internal Audit reports.

Confidential

TAX-#30312822-v1

POL00401629

Appendix 2

- See NRF's privileged legal advice memo.

Confidential

TAX-#30312822-v1

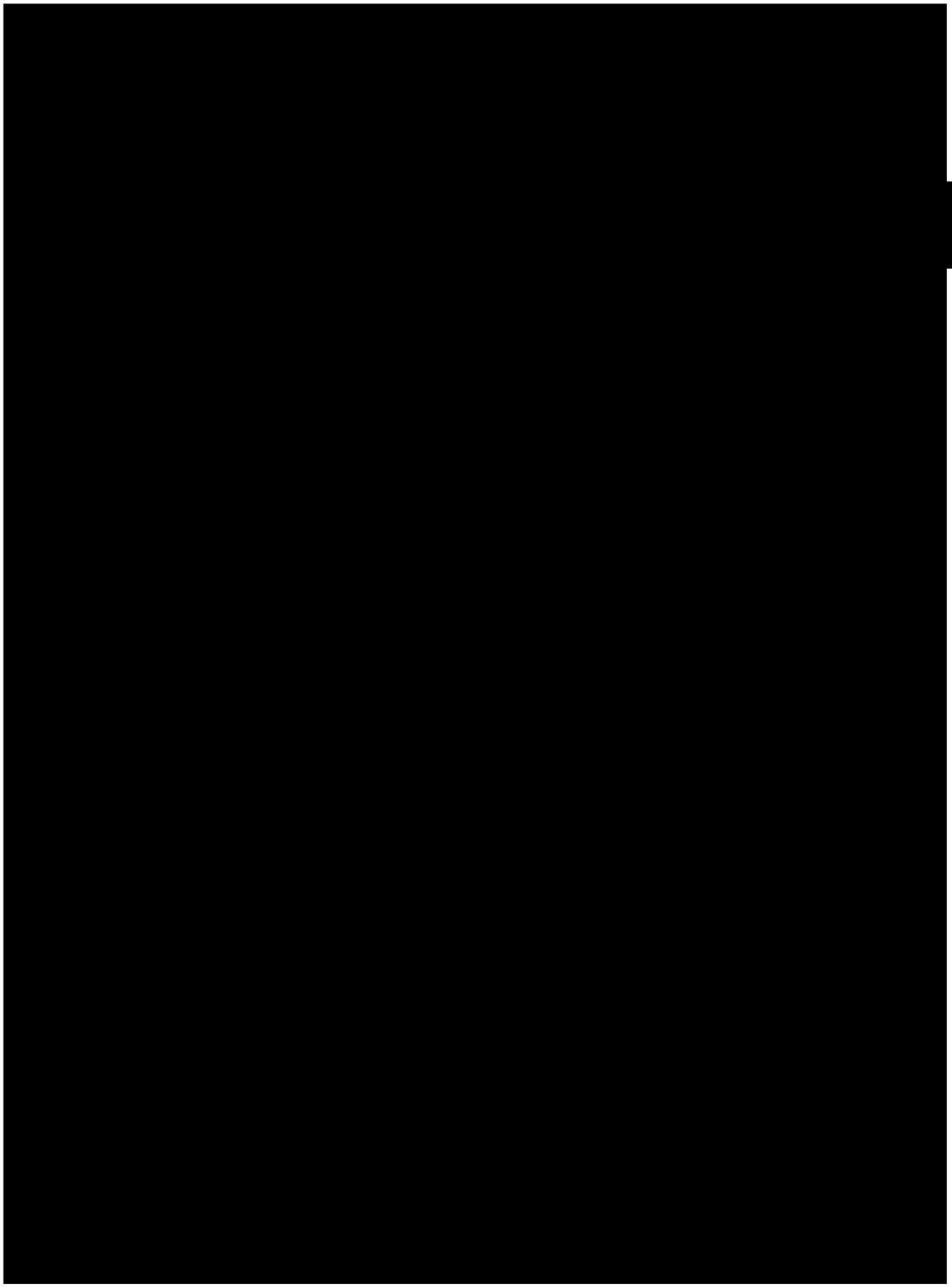
POL00401629

Appendix 3

- See attached r IRRELEVANT

Confidential

POL00401629



POL00401629

NORTON ROSE FULBRIGHT

[redacted]

4

POL00401629

NORTON ROSE FULBRIGHT

[redacted]

4

POL00401629

NORTON ROSE FULBRIGHT

[redacted]

4

POL00401629

[redacted]

4

POL00401629

[redacted]

4

POL00401629

[redacted]

4

POL00401629

POST OFFICE LIMITED
RRC REPORT

Title:	PCI DSS Compliance	**Meeting Date:**	10th September 2020
Author:	Joseph Moussalli, PCI DSS Programme Manager	**Sponsor:**	Jeff Smyth, Interim Group Chief Information Officer

5

Input Sought: For Noting

RRC is requested to note:
What programme progress has been made during the last reporting period?
What are the key risks?

Previous Governance Oversight

ARC has requested a rolling update on PCI-DSS programme progress.

Executive Summary

The programme consists of 2 core delivery streams:

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

The P2PE workstream is on track to deliver per plan the Vocalink accreditation of the retail & banking software. This activity is followed by a final round of testing and branch piloting activity which is on track to complete by March 2021. After the pilot activity is completed, the solution will be progressively rolled out across all branches with a full rollout and formal independent QSA accreditation being completed by June 2021. The team is continuing to investigate options to improve the velocity of the roll-out phase timelines.

The TOM workstream has identified seven areas where changes to products and processes are required to achieve PCI compliance. The activity required to address each of these areas has been planned and we are working with suppliers to achieve the required remediation.

Key updates in the last period:

- Fujitsu and Ingenico completed the 2nd banking key milestone, a balance enquiry, and the banking solution is on track to complete to plan.
- Delivery of the payment solution has slipped 3 weeks due to issues with the Global Payments test environment. Accreditation of the retail payment solution is now scheduled to complete in October (versus September). As this is not on the critical path there is no impact to the end to end plan.
- Additional changes have been identified and the project team is working with the business to understand criticality and potential workarounds. Fujitsu and Ingenico are also impact assessing the changes in order that these can be delivered in future releases of the software.

Confidential

POL00401629

- Finances: We are currently tracking within the 2% tolerance on the £15.8m approved at board. However, some new risks have been identified that may need additional funds.
- High Level Design now v2.4 has been updated with further TOM solutions.

Questions addressed

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

Report

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

IT workstream

- The Fujitsu / Ingencio software development is tracking to our overall IT workstream plan and CWO.
- Payments Release - there are two interim milestone delays that are being managed.
  - Payments release accreditation - Ingenico has started Global Payments accreditation and it was due for completion in 20th August 2020. It is now due for completion on 18th September 2020 with the certificate to follow in October.
  - The Fujitsu Payments release is tracking 3 weeks late on the contracted interim milestone 23rd October 2020 due to the complexity of the solution and key Fujitsu staff being affected by Covid-19. This is now due to complete on 16th November 2020. Neither of these changes affects the overall delivery critical path.
- Banking Release- Ingenico have delivered the 1st key milestone and 2nd key milestone in July (a demo of a Balance Enquiry). This milestone validates a significant proportion of the messaging protocols, transaction logic and connectivity paths between Ingenico and Vocalink.
- The upgrade of the Pin Entry Device (PED) to branches restarted on 1st July and we have now completed 95% of the branch upgrades (22,296 of 23,483 PEDs). This work is now due to complete in September 2020 with no impact to the critical path.
- POca – JPMorgan have started the design work to migrate to the banking framework.
- Good progress has been made with the Service contract with no major issues outstanding. This is activity is on track to work through formal governance and sign off is expected in September 2020.
- A standing executive meeting now occurs every 6 weeks with Executives from both POL (Nick Read & Jeff Smyth) and Ingenico (Dan Martensson, VP Global Enterprise Sales & Regional Marketing, and Paula Felstead, Global CTO). Ingenico continue to provide commitment to achieve full accreditation with Vocalink by the end of December 2020

Target Operating Model (TOM) Workstream Update

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

Confidential

POL00401629

- The TOM workstream is progressing to plan. A dashboard illustrating the status of the seven releases can be found in the Appendix 2. Key achievements this period are listed below:
- High Level Solution Design HLD v2.4 has been approved by EAG. It includes solutions Card Data Handing Environment (CDHE), Office 365 and Mimecast functionality received EAG approval, TES, PODG.
- Release A: Obfuscation of PCI data on screens and receipts. The solution for this has been developed been deployed.
- Release B: Telephone payments. The build has been completed ahead of schedule and the system is being tested.
- Release F (Quatrix): 14-day retention policy implemented on Quatrix. First Quatrix scan completed (14/08). Results currently being reviewed. Mimecast (risk raised last month) a way forward has been agreed on how to implement alerting rules.
- Release G: PCI DSS compliant solution agreed with EAG for providing full PAN for the Financial Crime and Banking enquiries team.
- Success Factors: Support and Support Plus training modules were released onto Success Factors for Information Security and Data Protection to incorporate PCI DSS training requirements.
- Change Giving: Change giving has been confirmed as out of scope as Change Giving cards are not on card schemes.
- HLSD: HLD v2.4 including Card Data Handing Environment (CDHE), Office 365 and Mimecast functionality received EAG approval (13/08)

2. What are the key risks on the programme?

The following are identified as key risks:

Risk: There is a risk that any changes needed to the Fujitsu/Ingenico software will impact the plan. Fujitsu and Ingenico have given a commitment to meeting the current timescales on the basis of no further changes.

Mitigation: Post Office continue to review design documentation and interim software releases to validate requirements traceability. A number of items have been identified and these are currently under review and under impact assessment with the suppliers. Where new requirements are identified an impact assessment will be completed to include any impact to time and cost. We are also seeking to manage business processes ie.e adjust operational processes to avoid any further critical path software development where applicable.

Risk: There is a risk that due to the complexity of the solution further funds may be needed. Fujitsu are forecasting an overspend of 10% - £504k.

Mitigation: Post Office are reviewing (and challenging) the forecast with Fujitsu and will continue to track and manage this risk with Fujitsu.

Risk: There is a risk that Santander cannot migrate services to route through Vocalink within the timescales.

Mitigation: Post Office team is working closely with Santander to produce proposals including costs and timescales. However, Santander have failed to provide a technical resource to scope out their changes. This has been escalated to the Director of Banking Services. A contingency technical arrangement is also being investigated.

POL00401629

Risk: There is a risk that Coronavirus may impact the delivery timescales for any supplier across the entire PCI programme. The outbreak of Coronavirus is a global risk event and the overall impact for the programme is not fully evaluated. Consequently, there may be a delay to the some or all of the agreed deliverables which could affect the build or deployment programme stages. Our risk assessment activity has been expanded to include the potential impact of any remediation work that has a high dependency on Indian offshore resources and in parallel, evaluation of how any second spikes could influence our delivery or implementation timetable.

Mitigation: Post Office is working with all engaged suppliers to better understand their contingency plans to ensure that delivery momentum is maintained. This includes the examination of options to minimise delivery impact by understanding key delivery person risks, supply chain risks and other indirect or latent dependency factors.

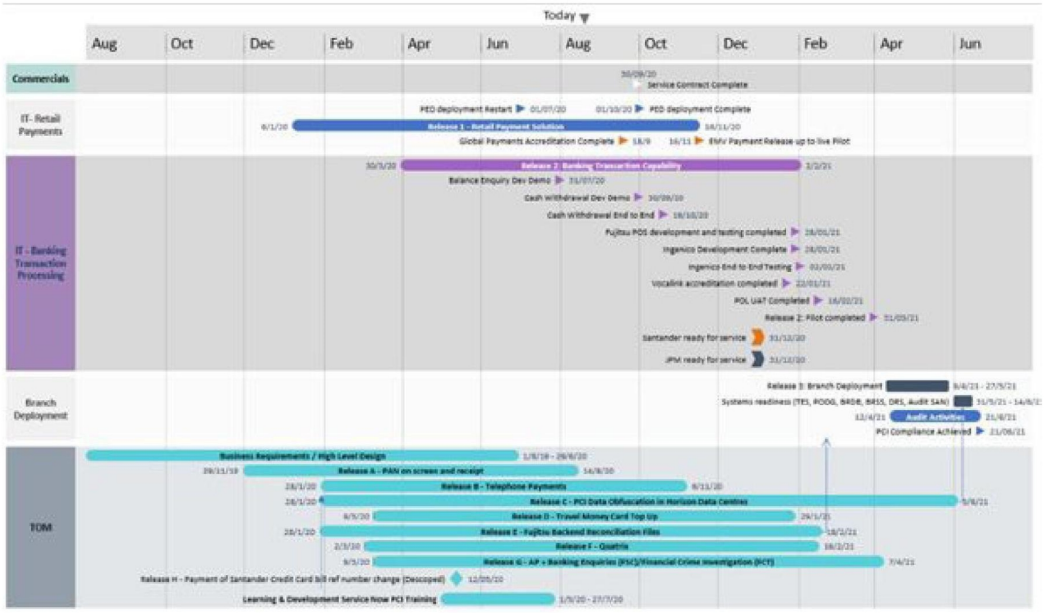
Confidential

POL00401629

5

Appendix 1

Programme plan

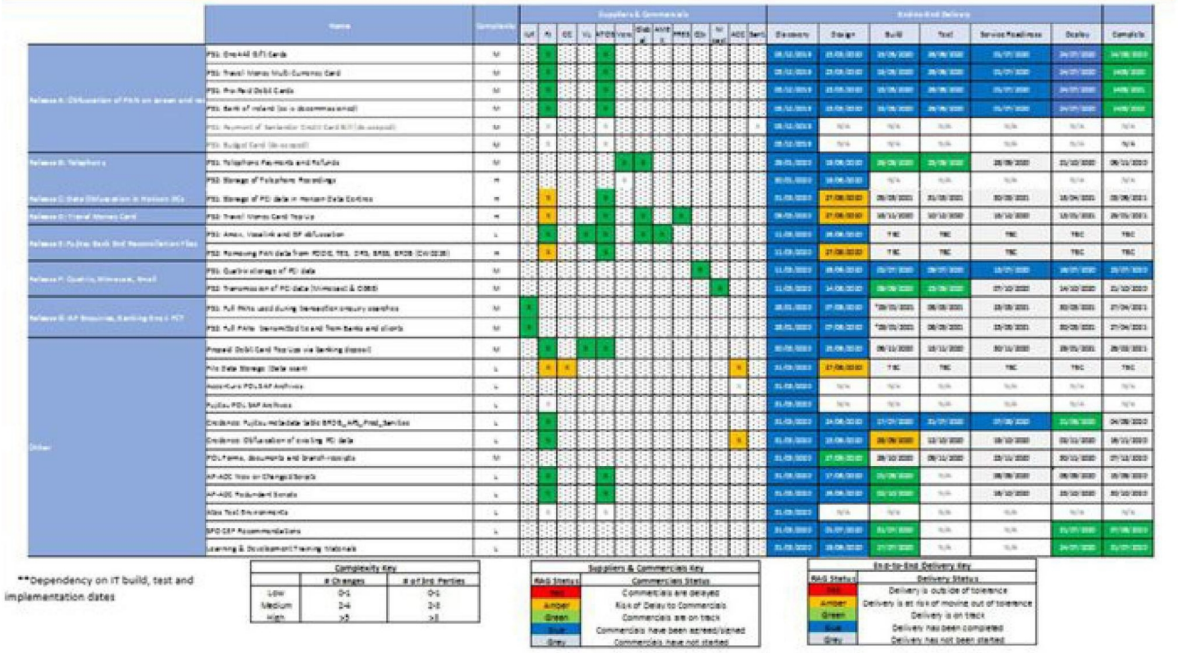


5

POL00401629

Appendix 2

TOM Workstream Dashboard



**Dependency on IT build, test and implementation dates

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

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

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

Confidential

POL00401629

Appendix 3 Finance Summary

PCI Programme Capex & Exceptional Spend (2018-2022)	Spend To Date (Incl. Apr-Jun 2020)	2020/21 (F/Cast) (Apr'20-Mar'21)	2020/21 (F/Cast) (Jul'20-Mar'21)	2021/22 (F/Cast)	LIFE
		FY	FY	FY	LIFE
Internal Labour	IRRELEVANT				
External Labour					
3rd Party Costs					
Exceptional Costs					
Actual / Forecast					
3rd Party Costs Comprise					
Fujitsu	£3,426,284	£5,587,244	£4,116,176	£546,556	£8,089,016
Computacenter UK Ltd	IRRELEVANT				
Atos					
Vocalink					
Other / TBC					

Confidential

POL00401629

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

Title:	Cyber Update	**Meeting Date:**	10 September 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

5

Input Sought: Noting

- To note the status and plans regarding the reduction of risk associated with Cyber Security

Previous Governance Oversight

- Rolling item in each RCC

Executive Summary

The COVID-19 period has required us to keep a close watch on cyber issues. As we enter the period beyond the initial COVID19 lockdown the cyber threat is changing and therefore continues to be a major focus for the IT team. This paper describes:

- How we plan to increase the maturity of our cyber capability in response to future threats and the emerging business and IT strategies;
- How effective we are at detecting and stopping current threats by understanding (through a dashboard) the nature of the threats we face and the value delivered by our SOC through a recent exercise;
- How we are dealing with the rising and changing threat from Ransomware.

Questions addressed

1. How are we planning to increase the maturity of our cyber capability?
2. How are we detecting and stopping current threats?
3. How have we focusing on and dealing with Ransomware-related threats?

Confidential

POL00401629

Report – How are we planning to increase the maturity of our cyber capability in 2020/1

4. At the last meeting we presented the results of the Deloitte maturity re-assessment which showed
    a. We had made significant improvements in most areas;
    b. That there are additional maturity improvement activities that we need to take to meet our agreed target maturity in 17 areas.

    This assessment considered our stated crown jewel systems and the external and internal cyber threats against them.

5

5. Since then the POL business and IT strategies have been developing at pace. These contain major strategic initiatives requiring enhanced Cyber attention, namely:

    a. **End User Computing** (EUC) delivering key cyber capabilities out of the box into our back-office environment;
    b. **Belfast Exit**, requiring the development of cyber capability into the Amazon Web Services cloud;
    c. **Strategic Platform Modernisation** (SPM) developing the next generation retail systems for POL all requiring security input
    d. **Joiners, Movers, Leavers** (JML) – securing the digital identity and access rights of POL staff
    e. **IT Controls** – increasing the coverage, effectiveness, and ownerships of controls across IT in Post Office Group and its third parties
    f. **Development of a GLO IT forensics team** within Cyber/IT

6. Item d is the subject of a separate paper from the CISO. Items e and f are being led by the CISO initially whilst permanent resources are recruited and will be reported elsewhere. Items a to c are covered in the programme for Cyber Maturity in 2020/1.

7. In common with many businesses POL is under significant cost pressure. Taking all of the above into account we have therefore adopted the following principles for our 2020/1 cyber programme:

    a. Deliver maturity increases where there is greatest value for lowest cost – this will include Cyber Strategy and Policy developments plus other areas where we are making process-related changes.
    b. Align as much as possible of the major cost items with delivery from other IT projects such as EUC, Belfast Exit where we will gain the capability as part of these projects.
    c. Defer the remainder of the higher cost items for maturity increase.
    d. Focus on security activities to enable the business such as those around SPM and Belfast Exit.

Confidential

POL00401629

8. Our 2020/1 cyber programme therefore consists of

   a. Cyber Capability maturity enhancements
      i. Deployment of Vulnerability Management automation within the SOC using Archer
      ii. Integration of SOC and IT Service ticketing through Service Now
      iii. Enhancements to SOC automation platform
      iv. Other Deloitte maturity review remediations
      v. Red team remediation activity
      vi. Enhanced Cyber Risk Management
   b. EUC-programme dependent deployment
      i. DLP phase 2 blocking capability
      ii. Office 365 event logging plat form through Microsoft Sentinel
      iii. Licence Cost avoidance by incorporation of built in Microsoft security tooling
   c. SOC enhancements, cost coverage and cost reduction
      i. Coverage of Belfast exit
      ii. Insource of Verizon capability
      iii. Rightsizing and organisation development
   d. SPM security requirements and delivery

9. From our original plans we have deferred several capabilities until beyond the end of FY2021– all of which are recommendations in the Deloitte Maturity assessments:

   a.
   b.
   c.
   d.
   e.
   f.
   g.

IRRELEVANT

10. Additionally, on target maturity levels, our Central risk team is presently revisiting cyber risk appetite statements considering COVID working practices, the relaxation of certain controls for extensive remote work practices and the reduction in capex. Changes in risk appetite will necessarily result in changes to target maturity of cyber capabilities as they are linked. Any necessary changes will be reported at the next meeting.

Confidential

POL00401629

Report - How are we detecting and stopping current threats?

11. For a 1-month period (15th July – 15th August) the Security Operations Centre (SOC) have completed a tabletop exercise of how we would cope without them – i.e. assume that the SOC is not there – what would we have missed.

12. The impact would have been
    a. No proactive monitoring of several threat management systems that maintain our enforcements through 100+ digital polices that are outside tower agreements – we would miss all threat alerts
    b. A varied range of security events, on average 30 events per day, 600 events over the period
        i. 150 Phishing attempts
        ii. 20 Malware attempts
        iii. 50 Vulnerabilities
        iv. 30 Firewall rules improved
        v. 60 investigations for policy breach (insider threat)
        vi. 40 Network attack attempts
        vii. 240 Threat intelligence assessments to brand and banking

13. Major investigations – high severity incidents include;
    a. (DLP) Detected Asset with sensitive data with minimal access controls
    b. (DLP) Employee Mass File delete detected, subsequent disciplinary proceedings followed
    c. (DLP) Detected user sending to personal mail, Data Breach recorded with DPO
    d. (Phishing) Care Home phishing campaign, POL user compromised, Device isolated and threat remediated
    e. (Malware) User downloaded compromised file containing Malware, Device and user account treated and threat remediated
    f. (Threat Intelligence) 250 + events of detection and remediation, reports to brands and banking provided, including details passed by to Capita

14. Lessons learned from this tabletop exercise:
    a. EUC provider will only process Malware events under contract SLA (this has been 4 days in previous cases), POL SOC to take immediate action to resolve.
    b. DLP is a major element of the daily incident count and requires constant monitoring with POL business teams frequently operating outside information security policy (DLP Phase 2 "analysis and pre enforcement activities" will provide the analysis to the business to conduct an operations policy review in Q4)
    c. Attacks to our brand are constant and increasing, SOC provides this service as this is outside any tower contract
    d. POL SOC is operationally maxed out with current threat and incident volumes
    e. More Security Integration Event Management (SIEM) data ingestion is required to widen the threat intelligence capability

5

Confidential

POL00401629

15. Appendix A shows the statistics that the SOC gathers on a regular basis and the dashboard that we are using to drive the operational aspects of our work. At each of our following meetings we will publish a dashboard for this forum covering key cyber metrics of interest and the trends we are seeing.

Report – Ransomware

16. Ransomware attacks through the COVID period continued to increase in number and sophistication. The recent issues faced by Travelex and their inability to rapidly recover operations and reputation from a serious ransomware attack are a good example. Other attacks continue on an almost daily basis.

17. Against that backdrop we asked Deloitte to help us by assessing our readiness for a ransomware attack and to develop a playbook so that in the instance that we had such an attack then we would be able to respond accurately and quickly.

18. The incident playbook has now been fully integrated into the incident process and this is now fully aligned to the IT Major Incident Management process.

19. Further enhancements later this year will see the SOC move its incident ticket management system to "ServiceNow" with full resolver group integration with the rest of the IT service organisation. This will further increase our speed of response to ransomware

20. This change also supports the security operations integration with the "Cloud Centre of Excellence" for AWS onboarding of Horizon architecture.

21. Our next steps in this area will be to share and compare with our key 3rd parties.

Confidential

POL00401629

Appendix A, Page 1

Threat Landscape (Cyber Perspective)

IRRELEVANT

Vulnerabilities (Accenture and CC)

IRRELEVANT

Horizon - Fujitsu; - High number of vulnerabilities discovered each quarter
- Due to legacy and aging infrastructure risks have been accepted by way of PCI-DSS process/certification
- Scan only covers PCI-DSS scope

Scan only processed on a quarterly basis as per contract

IRRELEVANT

Security Posture

IRRELEVANT

Phishing Protection (AI and SOC)

IRRELEVANT

IRRELEVANT

Confidential

POL00401629

Appendix A, Page 2

POL Security Operations Centre Ticket Mgmt

IRRELEVANT

HIGHLIGHTS OF THE MONTH - (July 2020)

IRRELEVANT

Mail Filtering

Insider Threat

IRRELEVANT

Confidential

POL00401629

Appendix A, Page 3

Covid-19 Tracked Major changes

IRRELEVANT

All testing on Horizon equipment is undertaken from physically secure supplier locations	Testing of Horizon changes to be undertaken on existing devices moved to Atos and CC users' homes	Although access to conventional testing locations is no longer possible where strong physical controls are in place, devices are secured by process/guidelines. This remains in place and is facilitating the continued testing for releases.

Change Assurance

IRRELEVANT

PCI DLP Trends

IRRELEVANT

Number reviewed False Positives

Assurance Actions

IRRELEVANT

ISMF Actions

IRRELEVANT

Confidential

POL00401629

Appendix B – 2020/1 Cyber Programme

IRRELEVANT

9

POL00401629

POST OFFICE LIMITED
AUDIT & RISK COMMITTEE

Title:	JML Update	**Meeting Date:**	10 September 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

5

Input Sought: Noting

- To note the status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML) – in particular those associated with Leavers during the current hybrid operating model

Previous Governance Oversight

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

Executive Summary

In our continued focus on Joiners, Movers, and Leavers we have performed a deep dive on the Leavers process, as it is likely to present the most risk to the business. Our analysis covers the period for which COVID-19 has been active as this has immediate relevance to the operating model and challenges facing the business in the next few months. Short term and longer-term actions are included. Subsequent papers will continue this analysis but will also expand the focus to cover Joiners and Movers and other areas within Post Office Group.

Questions addressed

1. What are the complexities we need to address associated with the leavers process?
2. How well have we managed these complexities during the COVID-19 period from March to July 2020?
3. What is the action plan?
4. What are the additional activities from a control's perspective around leavers?

Confidential

POL00401629

Report – Joiners, Movers and Leavers (JML)

5. In this report we are focusing in on the Leavers process for staff and contractors as this presents the greatest risk to the business. Additionally, we expect there to be more leavers than there are joiners and movers in the next 3-6 months, increasing the need to focus on this process.

5

What is the Leavers process and what are the complexities associated with it?

6. The leavers process is shown in Figure 1.

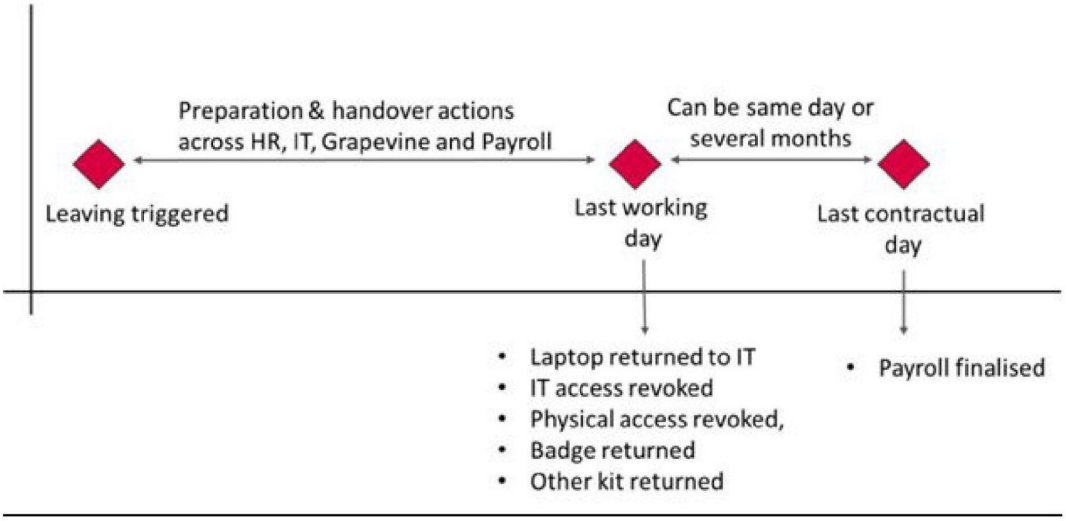


Figure 1 Leavers Process

7. The process is made more complicated by the following factors:

   a. There are different types of leaver that the process must take account of which have implications for the risks and mitigations needed:

      - ***Standard leavers*** initiated by an individual moving role outside of Post Office or for example through retirement.
      - ***Extraordinary leavers*** – For example, those who leave through a compromise agreement or redundancy arrangements.
      - ***Rapid leavers*** – such as those who exit in response to a disciplinary issue.
      - ***Health-related leavers*** – for those who have been long term sick for over 2 years or in extreme circumstances through death.

Confidential

POL00401629

b. There are different ways it can be triggered
   i. Individuals trigger the process by resigning via a resignation letter to their line manager. It is the line managers responsibility to lodge this on Success Factors which initiates the leaving process through the HR Service Centre.
   ii. Alternatively, the organisation can trigger the leaving process directly on Success Factors which is handled by HR.

c. Actual leave dates can vary - The contractual and final working dates for individuals vary as many people leave and take holiday within their notice period. Others are exited rapidly with gardening leave. Therefore, the date at which access gets turned off for someone will vary from the actual contractual leaving date.

8. These complications introduce extra risk into the process and are therefore a necessary part of handling it.

How well have we managed the Leavers process during the COVID-19 period from March to July 2020?

9. To gain insight into how well the Leavers process has worked during lockdown we have:
   a. Logged all staff and contractor leavers during the COVID-19 virus from March to July 2020 – there were 184 in total;
   b. Cross-matched the leavers data with that held for IT access, returned laptops, building access and payroll;
   c. Interviewed those who are responsible for running the various elements of the process to understand their experience with it;
   d. Drawn conclusions from this activity which highlights how well we have performed and where we need to do better.

10. What went well:
   a. **IT access for all leavers was removed on time.** There were 6 people who had in theory left but still had access available. On closer inspection those 6 were contractors who had been converted to permanent roles – explaining why they were simultaneously in the leaver list but also still active. The synchronisation between Success Factors and IT access systems therefore appears to be working well. We propose to perform a deeper dive on data across the whole of JML to further back this up.
   b. **The HR leaving process was in all cases started on time**. HR confirmed that all leavers were made known to HR in a timely fashion. This is critical to the success of the process. The message is getting through to Line Managers that they have a significant role to play. This will be reinforced ahead of the September OE review through further training for all Line Managers.
   c. **Physical access and payroll were also terminated correctly for these leavers**.

POL00401629

11. What needs improvement:
    a. **The process for return of laptops and other kit**. The leavers checklist makes no mention of the need to contact someone about IT kit collection which could result in line managers and leavers not returning kit. There is also no formal process for informing IT operations that someone is leaving under current working arrangements. This was easier when we all worked in a physical office as people had a physical reminder of where to send kit. Now we are working remotely then a newly initiated pickup by courier process is starting to have a good effect. As IT have no formal notification the need to pick up kit then a closer join up between IT and HR would help. This could be achieved through linking the HR and IT service desks together.
    b. **Some leavers have deleted and downloaded confidential data**. During this period, our DLP platform noticed some above threshold patterns around document access for certain leavers. In all cases accounts were locked pending investigation of the severity of each case. For three of these there was a need for further coordinated action by Cyber, HR and DPO. There needs to be clearer guidance on the leavers checklist to cover what to do (and what not to do) with data when leaving, even though this is already covered in policy documentation.
    c. **Core data issues seen**. During this initial analysis there were glimpses of issues surrounding cleanliness of data in HR and IT systems. The systems appear to be working but the question remains are their further issues lurking due to the state of the data. We will perform a deeper dive and clean up of this data if needed.
    d. **Gaining access to data on JML for analysis**. This has been surprisingly difficult as POL do not have ready access to data – we need to raise requests to go to 3rd parties which has an associated time delay with it and in some cases cost implications.

What is the leavers action plan?

12. In summary our action plan is as follows
    a. Update the Leavers Checklist and Line Managers guidance to include IT kit return and data guidance for leavers [September 2020];
    b. Implement a join up of HR and IT service desks [October 2020]
    c. Explore ways to speed up data access [October 2020]
    d. Perform a full analysis of all data across Success Factors and IT to ensure they are in sync and accurate – [September to December 2020]
    e. Expand analysis to Joiners and Movers – [November 2020]
    f. Recruit a JML analyst for IT to further investigate data [September – October 2020]

Confidential

POL00401629

What are the further actions we are taking around JML?

13. We are going to designate two new responsibilities for JML: IT System Platform Owner (SPO) responsible for the IT elements of a platform and a Business Data Owner (BDO) from the owning business who are accountable for the data in each system. Each of these roles will have a lock-step role in managing JML as described below.

14. We will produce a monthly dashboard for the GE which will show all leavers by function. There will be a three way sign off on this dashboard for each leaver from IT, HR and Line Manager to assert that all necessary leave-related activities have been completed.

15. For movers we will perform a quarterly sweep by SPO and BDO to positively confirm:

    a. What access people have had
    b. What access people should have going forward

    This will be prioritised for the top platforms initially

16. All privileged access for IT systems will be approved by SPO, CISO and CIO in addition to the current process.

17. For key third parties, including Fujitsu, Verizon, Accenture and Computacenter we already receive attestation of JML and Privileged Access Management on either a monthly or quarterly basis. We will move this to monthly in all cases bearing in mind that this may require contract adjustments. We will also add Ingenico to this list. As a next step we will introduce spot auditing alongside attestation to increase the assurance level of this activity.

18. On movers we are going to focus on our top 5 systems and for each we will validate the movers process has the ability to tear down and build up access for movers, thereby ensuring that access is not carried from one role to another.

19. The Deloitte Maturity assessment reported at the last meeting has made specific recommendations about identity specifically focusing on the need for automation. We will add these to our Cyber programme subject to funding approval.

20. Our COBIT 5- based controls framework covers JML. These controls are under review as part of the enterprise-wide controls review under Legal and Compliance.

21. There is an internal audit review scheduled for Q3/4 of 2020. Terms of reference are being developed now.

Confidential

POL00401629

Post Office Insurance Renewal – Process Update

Author: Mark Dixon Sponsor: Brian Kelly Meeting date: 10 September 2020

Executive Summary

Context

6

The business has a series of insurance policies due for renewal on IRRELEVANT A summary of the insurance programme in place at renewal in IRRELEVANT is set out in Attachment 1 together with the insurance premiums paid in Attachment 2. Given the timing of the RCC meeting and the timetable for renewal we are not able to provide a detailed update at this time. This paper provides a brief outline of our approach for the 2020 renewal and sets out a number of things that may impact renewal.

Question addressed in this report

What is the renewal process for 2020?
How does the renewal process for 2020 differ to previous years?

Conclusion

We believe that the approach adopted for the 2020 renewal will allow us to ensure we have IRRELEVANT
IRRELEVANT

Input Sought

The RCC members are asked to note the update on the 2020 renewal process

Strictly Confidential

POL00401629

The Report

What is the renewal process for 2020?

1. The 2020 renewal date is IRRELEVANT for all insurances.

2. For the IRRELEVANT renewals we followed a fully OJEU-compliant procurement process. The insurance market traditionally doesn't use an OJEU-type process. Hence we saw some success on certain lines and were able to r IRRELEVANT but on other more specialised lines, for example IRRELEVANT IRRELEVANT

3. In June 2020 we worked with Procurement (Antony Ray) and Legal (Ravi Mudundi) to decide whether an OJEU process was required for the 2020 renewal. Legal have concluded that, provided the broker (Lockton) was compliantly procured, which it was, then we do not need to go through another procurement exercise and we can simply instruct Lockton to secure the best policies for us. This is therefore the approach that we are taking for the 2020 renewal.

4. We will provide an update to the ARC in September and, given the timeline for renewal and company meeting dates, ask that authority to approve the final programme is delegated to the Chairperson and Group Chief Finance Officer.

How does the renewal process for 2020 differ to previous years?

5. Our primary focus has been on delivering an insurance programme at a reasonable cost to the business. For our IRRELEVANT renewals the overall insurance cost IRRELEVANT which was IRRELEVANT For the IRRELEVANT renewal we saw IRRELEVANT for IRRELEVANT and hence IRRELEVANT As a result, on a IRRELEVANT We also added IRRELEVANT IRRELEVANT so overall IRRELEVANT

6. Early indications are that conditions in the IRRELEVANT IRRELEVANT In addition, as a result of Covid-19 insurance market conditions in general are difficult. We are therefore expecting to see IRRELEVANT on IRRELEVANT for the 2020 renewal. The IRRELEVANT we put in place at the IRRELEVANT IRRELEVANT We are

6

POL00401629

exploring ways of IRRELEVANT as part of the renewal process.

Attachment 1: Summary of Insurance Programme at IRRELEVANT Renewal – see separate document.

Attachment 2: Insurance Premiums at IRRELEVANT Renewals

	Premium IRRELEVANT	Premium	vs Last Year (£)	vs Last Year (%)	Comments
IRRELEVANT					IRRELEVANT
Sub-total (excl IRRELEVANT					
IRRELEVANT					
Total					
IRRELEVANT					

6

POL00401629

Post Office Group - Summary of Insurances

(based on renewal at IRRELEVANT

Insurance Line	General	Deductibles / Retention	Limit of Indemnity / Sub-limits	Comments
POST OFFICE - GROUP INSURANCE COVERAGE	IRRELEVANT			

POL00401629

Tab 6 Corporate Insurance Renewal 2020/2021

Insurance Line	General	Deductibles / Retention	Limit of Indemnity / Sub-limits	Comments
	IRRELEVANT			
IRRELEVANT	IRRELEVANT	IRRELEVANT	IRRELEVANT	
	IRRELEVANT	IRRELEVANT	IRRELEVANT	
	IRRELEVANT	• .Various	• Various	

6

POL00401629

POST OFFICE LIMITED
COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	10 September
Author:	Sarah Gray (Legal Director)	**Sponsor:**	Ben Foat (General Counsel)

Input Sought:

Noting:

The Board is asked to note the new or proposed material changes to laws and regulations this month.

7

Previous Governance Oversight

Reported at each RCC & ARC

Executive Summary

There are 5 matters for the Committee to note (details of which are set out in the Appendix):

1. Court of Justice of the European Union (CJEU) - Schrems II Decision – the CJEU is tightening rules relating to transferring personal data to non-EEA countries using the Privacy Shield and contractual arrangements (so called model clauses). For the moment the risks to Post Office group is not significant because Post Office does not have many agreements containing model clauses. However, Post Office must ensure that its IT strategy takes into account how personal data is going to be transferred outside of the EEA and what counties Post Office will be comfortable with sending the data to.

2. Ofcom Consultation – Implementing the new European Electronic Communications Code – Ofcom is reviewing approach of the telephony providers to their customer, including fair outcomes, which may result in need for material changes to the way the telecoms firms will be allowed to provide their services. There is a risk to Post Office having to make changes that will impact its proposition significantly. The full extent of the code will be clear once Ofcom issues revised statements.

3. Online Platform Regulations – This B2B regulation forces providers of platforms such as aggregators websites (for example Confised.com) to provide its clients with information and tools allowing more balanced distribution of bargaining power between the provider and the client. Post Office and Post Office Insurance will be benefiting from these regulations as clients of aggregators websites.

4. Corporate Insolvency and Governance Act – The enactment of the Act has been triggered by Covid and the potential insolvency cases of suppliers of goods and services. The measures aim to: (i) afford companies some breathing space (moratorium) from creditor action; (ii) provide a space for restructuring compromise or arrangement without deepening financial difficulties; and (iii) restriction on suppliers from terminating contracts or supply, or insisting on payment of sums due where the client has entered into a relevant restructuring or insolvency process. Point (iii) applies to Post Office's contractual relationships with its clients and suppliers.

Strictly Confidential

POL00401629

5. HM Treasury consultation on new economic crime levy – A vehicle to raise approximately £100 million per year from entities regulated for Anti- Money Laundering purposes and support reforms to the sustainable resourcing of economic crime. Post Office is assessing if it should be subject to the levy.

Strictly Confidential

POL00401629

Appendix 1

1. Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
Court of Justice of the European Union ("CJEU") Schrems II Decision	Most organisations which transfer personal data outside of the European Union ("EU") rely on data transfer agreements (which adopt the Standard Contractual Clauses ("SCCs")), or for transfers to the United States of America ("US") the EU:US Privacy Shield Framework. These mechanisms address the requirement for adequate protection of data to the EU standard to be put in place for transfers. The validity of these mechanisms was brought into question before the CJEU.	On the 16 July 2020, the CJEU issued its final judgment that invalidated the EU:US Privacy Shield Framework as a transfer mechanism for transfers of personal data to the US, however ruled that SCCs are to remain valid. Although SCCs are still valid, the CJEU has set out a burdensome obligation that their use must be assessed on a case-by-case basis and due diligence must be undertaken on the country the personal data is being transferred to. The previous position was due diligence was only necessary on the importer of the personal data, not the country. The judgement also confirms that individual data protection authorities can revoke reliance on SCCs if they believe they won't be complied with.	Across Post Office there are only a handful of small contracts where Privacy Shield is being used, and even then, additional protection using SCCs was implemented; therefore no transfers are relying solely on Privacy Shield. The SCCs are being modernised and new versions should be available soon, coupled with promised further guidance from the European Data Protection Board on moving forward without Privacy Shield, this softens the immediate impact. A potential problem is that the use of SCCS for transfers to the US are unlikely to be seen as adequate given the CJEU were so critical of the US legal regime in relation to Privacy Shield. However, until guidance is provided by the European Data Protection Board there is some time for Post Office to address the impact fully. Until then the Post Office Data Protection Team are continuing to support the business areas with responding to any pushback from third parties in relation to SCCs and the necessary due diligence. A further and bigger concern is there is expectation that a third Schrems case will be brought to invalidate the use of SCCs all together. This isn't expected to occur for a couple of years and it is hard for Post Office to say what we could rely on instead at this time, however if this does happen it is likely another full remediation of contracts will be required.	The Data Protection team continue to work with external law partners to keep abreast of any developments and ensure these are built into any upcoming contracts. However for now those contracts that did rely on Privacy Shield have the SSCs as a valid mechanism of transfer and the work is mainly reactive. Chris Russell, our Data Protection Officer, has also met with ICO and been told they are also in the process of producing relevant guidance in addition to that provided by the European Data Protection Board. Further updates will be provided to the Law and Trends Forum as appropriate.	
Ofcom Consultation – Implementing the new European Electronic Communications Code ("EECC")	The EECC is an EU Directive that updates the regulatory framework for communications services which the UK is required (despite Brexit) to implement into domestic law by 21 December 2020. The EECC will apply to POL's provision of broadband and landline within the telecoms business.	COVID-19 has caused significant challenges for the communications industry, something which has been recognised by Ofcom in light of implementing the EECC. In light of these challenges, on the 7 May 2020, Ofcom published a statement that it would allow the industry 12 months from the date of the publication of its final statement in Autumn 2020 to implement the most	Until Ofcom publish the final statement on how the EECC will become domestic law there are still many questions that remain unanswered. Despite this, there is a real risk of the new measures having a material cost impact on the Telecoms business. The Compliance and Telecoms teams have been monitoring developments on the EECC and are working closely with Fujistu on implementing any necessary changes to ensure full compliance.	Ofcom intends to publish a statement setting out their decision on the measures in Autumn 2020. Both the Compliance and Telecom teams will keep abreast of any changes and any further obligations published by Ofcom. Post Office is assessing if to respond to the consultation.	

Strictly Confidential

POL00401629

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	Purpose: a new package of measures to protect broadband, mobile, pay TV and landline phone customers and help ensure they get a fair deal, which is designed to allow customers to shop around with confidence, make informed choices and switch easily. The EECC includes regulatory changes across a wide scope, including: - Provision of a 'Contract Summary' sheet to customers before they sign up; - Strengthening customers rights to exit mid-contract where there are contractual changes which do not benefit the customer; and - Easier switching for broadband and mobile customers.	onerous measures introduced by the EECC. Ofcom have since published a further consultation on two revised proposals in July and have invited responses by 11 September 2020. Compliance will be necessary once the EECC is adopted into UK law.		Further updates will be provided when appropriate.	
Online Platform Regulations	The European Commission has taken steps to redress a perceived imbalance between online platforms and the businesses which provide goods and services on them by introducing the Online Platforms Regulation ("OPR") that has been in force since 12 July 2020. OPR regulates business to business practices and POL (and POMS) as the clients are the beneficiaries of the OPR.	The OPR is applicable to online platforms, marketplaces, apps stores and social media platforms, such as MoneySupermarket or Confused.com (OP Providers). The OPR introduces a ban for the OP Providers on carrying out certain unfair practices for example, suspension or termination of an account without clear reasons, failure to provide contracts in plain and intelligible language, and failure to give adequate notice for changes to contracts. Other measures include: - Transparency requirements in relation to the parameters used to rank goods and services on their site; - Disclosing any advantage given to their own products over others;	Post Office and POMS will be benefiting from the changes because they are the users of aggregator websites for some products, such as insurance or loans. Post Office and POMS will gain greater transparency and rights within its agreements with OP Providers.	Post Office has already seen some aggregators making contact with amended terms to ensure compliance with the OPRs and will continue to engage. In addition, Post Office has been proactively asking aggregators whether their terms reflect the provisions of the OPR and is ensuring this is captured in negotiations regarding future contracts. Legal are also to reach out to the Telecoms team who are using OP Providers to ensure alignment and support is provided.	

Strictly Confidential

POL00401629

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		- Introducing an internal complaint handling procedure; - Proposed modifications of terms and conditions must be provided to the business user on a durable medium; and - Notice of changes with supporting details and considerations. -			
Corporate Insolvency and Governance Act ("The Act")	The Corporate Insolvency and Governance Act 2020 makes the most significant changes to UK insolvency law for nearly 20 years. Key measures achieved Royal Assent on the 25 June 2020.	The Act introduces three new permanent measures: 1. A new free-standing moratorium; 2. A restructuring plan process; and 3. Restrictions on termination of contracts for the supply of goods and services. It also includes temporary measures (lasting until 30 September 2020) in response to COVID-19, which are: 1. Restrictions on using winding-up processes; 2. Temporary changes to wrongful trading rules; and 3. Relaxation of meetings and filing requirements to give companies greater flexibility. Extensive powers for the Secretary of State are provided to amend certain provisions; recognising that this is a complex piece of legislation introduced at speed and adjustments may need to be made to deal with issues that arise as the Act begins to be put into practice.	The Act provides useful additions to the restructuring process and welcome relief for distressed businesses. However, the most relevant measure for Post Office is the wide-ranging prohibition on the operation of termination clauses in contracts for the supply of goods and/or services where the counterparty enters a relevant insolvency process. These provisions apply where the relevant insolvency procedure commenced on or after 26 June 2020 and will apply in respect of contracts entered into before, as well as after that date. Under the new provisions, Post Office when acting as a Supplier will be prevented from: - Terminating a contract or doing 'any other thing' because the company has entered a relevant insolvency procedure; - Terminating a contract for breaches which occurred prior to the relevant insolvency procedure; or - Making it a condition of future supplies that pre-insolvency arrears are paid. It's worth noting that 'any other thing' is not specifically defined and is a particularly broad concept. The explanatory notes only provide one example of changing payment terms, but it is assumes that the wording will capture any exercise of a contractual right triggered upon an event of insolvency. Post Office will still be allowed to terminate the contract: - For the new breaches which happen after the insolvency procedure begins;	Post Office will need to review the existing position of key customers and identify those at risk where the termination clauses are narrow and Post Office could be bound to continue to supply services where a customer is in an insolvency situation with no guarantee of payment of arrears. Consideration should be given to whether there is scope, pre-insolvency for renegotiation of contracts. For future contracts where Post Office is the Supplier, drafting should ensure that any rights for Post Office to terminate where a customer is in an insolvency situation are widely drafted to ensure termination is possible before The Act provisions step in. (i.e. earlier triggers for termination). The Legal Team will take this forward and provide updates as necessary.	

Strictly Confidential

POL00401629

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
			- With the permission of the insolvency office holder or directors; or - With the permission of the court, provided the court is satisfied that continuation of the contract would cause Post Office hardship. The Act provides several exclusions such as Post Office's banking contracts, or contracts where we supply goods/services to another public sector entity may not be affected by the new measures. /		
HM Treasury ("HMT") consultation on new economic crime levy ("levy")	At the 2020 Budget, the Government announced its intention to introduce an economic crime levy. The levy aims to raise approximately £100 million per year from entities regulated for Anti-Money Laundering ("AML") purposes and support reforms to the sustainable resourcing of economic crime. Responses to the consultation are due by 13 October 2020.	The consultation invites views on how the levy could operate in practice to ensure that it is proportionate and effective, however doesn't look at the merit of introduction of a levy. The views sought include what the levy will pay for, how it should be calculated and distributed across the AML sector and how the levy should be collected. Current proposals include, but not limited to, a levy based on a percentage increase of current AML fees paid, the size of a business, the number of employees or the number of SARS raised.	Post Office already pay around £2million in HMRC fees as well as additional Fit and Proper costs. An economic crime levy will only increase the amount of money due to HMRC, and unless Post Office can find a reason to object it is likely that we will be affected. Until HMT publish exactly how the levy will be calculated, there can be no estimate on how much Post Office would be expected to pay if and when the levy is formally introduced.	Post Office intend to respond to the consultation and the Financial Crime team are working with Legal to review the consultation as well as look into whether there are any reasons that can be raised to argue that Post Office shouldn't be subject to the levy. Further updates shall be provided as appropriate.	

Strictly Confidential

POL00401629

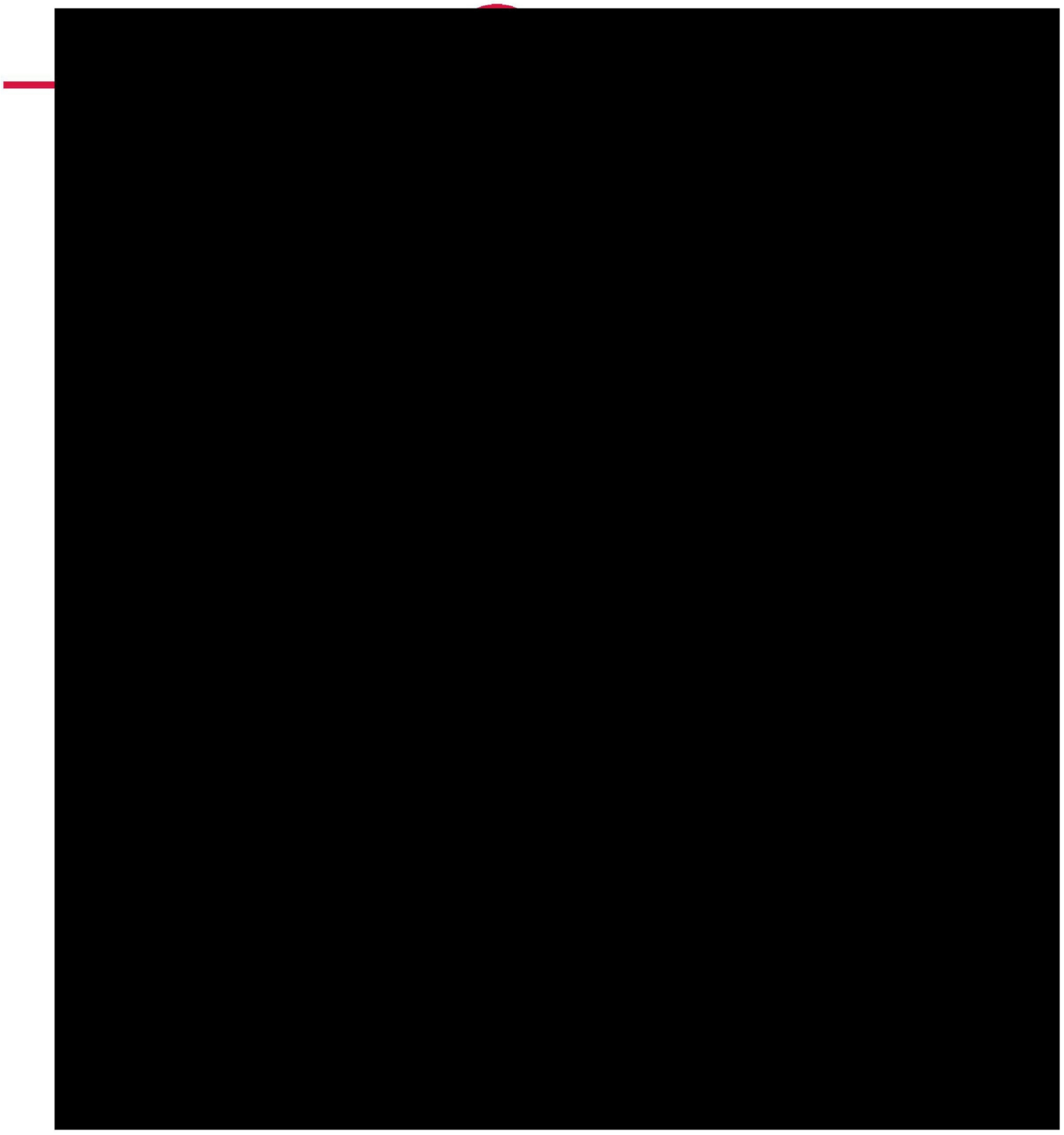
POST OFFICE LIMITED RCC REPORT

Title:	**H1 Legal Risk Report 20/21**	**Meeting Date:**	**22 September 2020**
Author:	Sarah I. Gray, Group Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

[redacted]

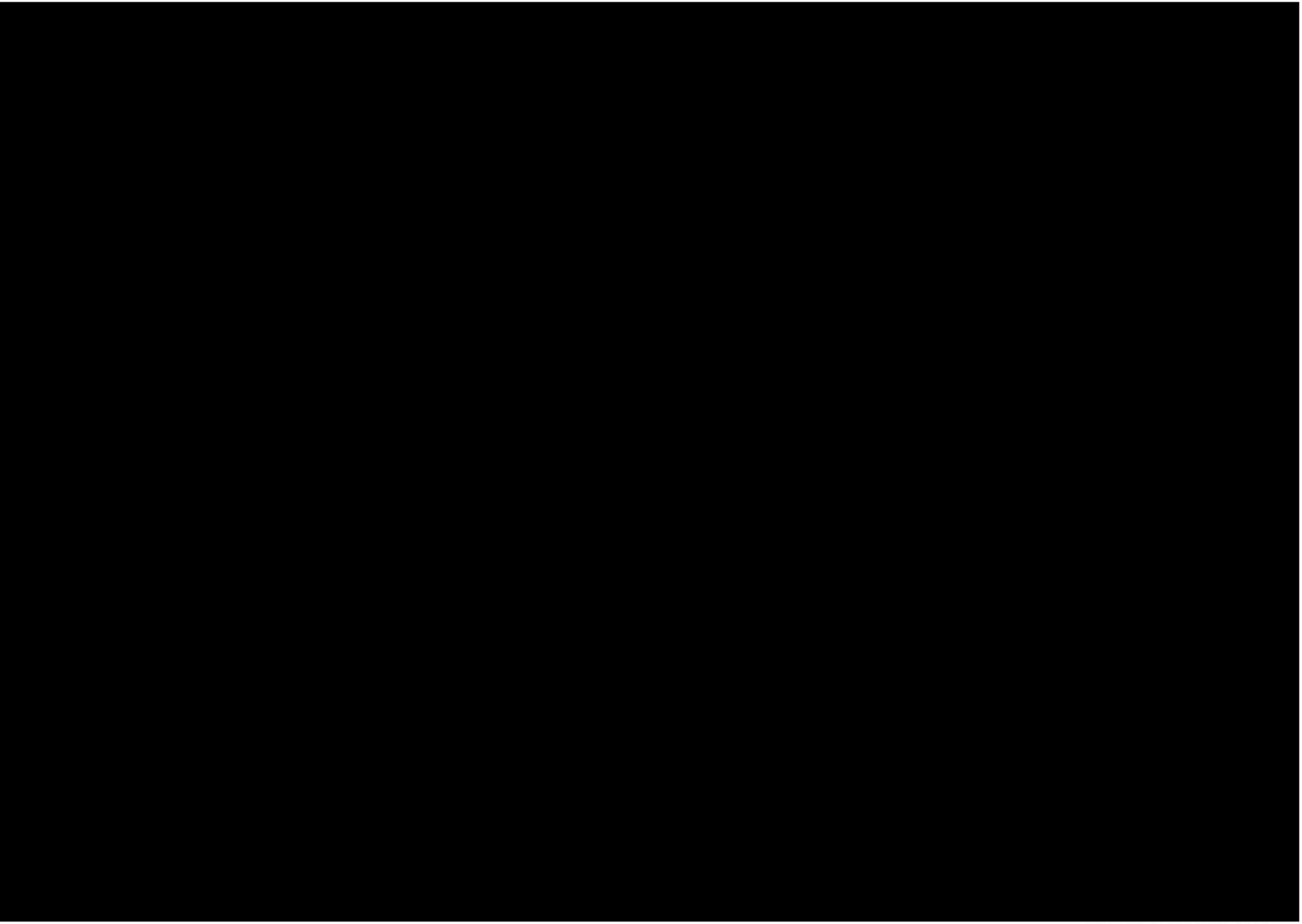
8

POL00401629

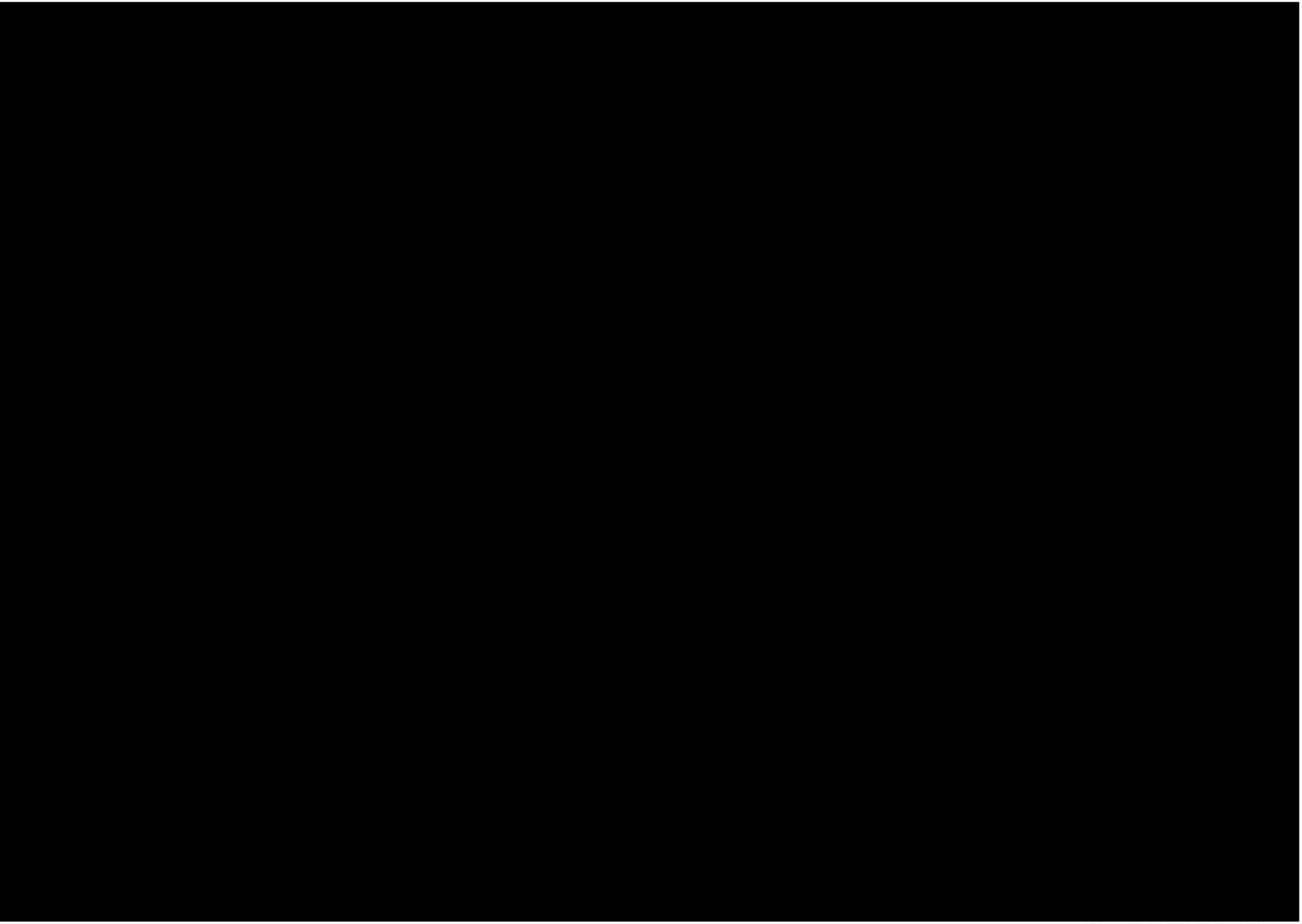


Strictly Confidential & Legally Privileged

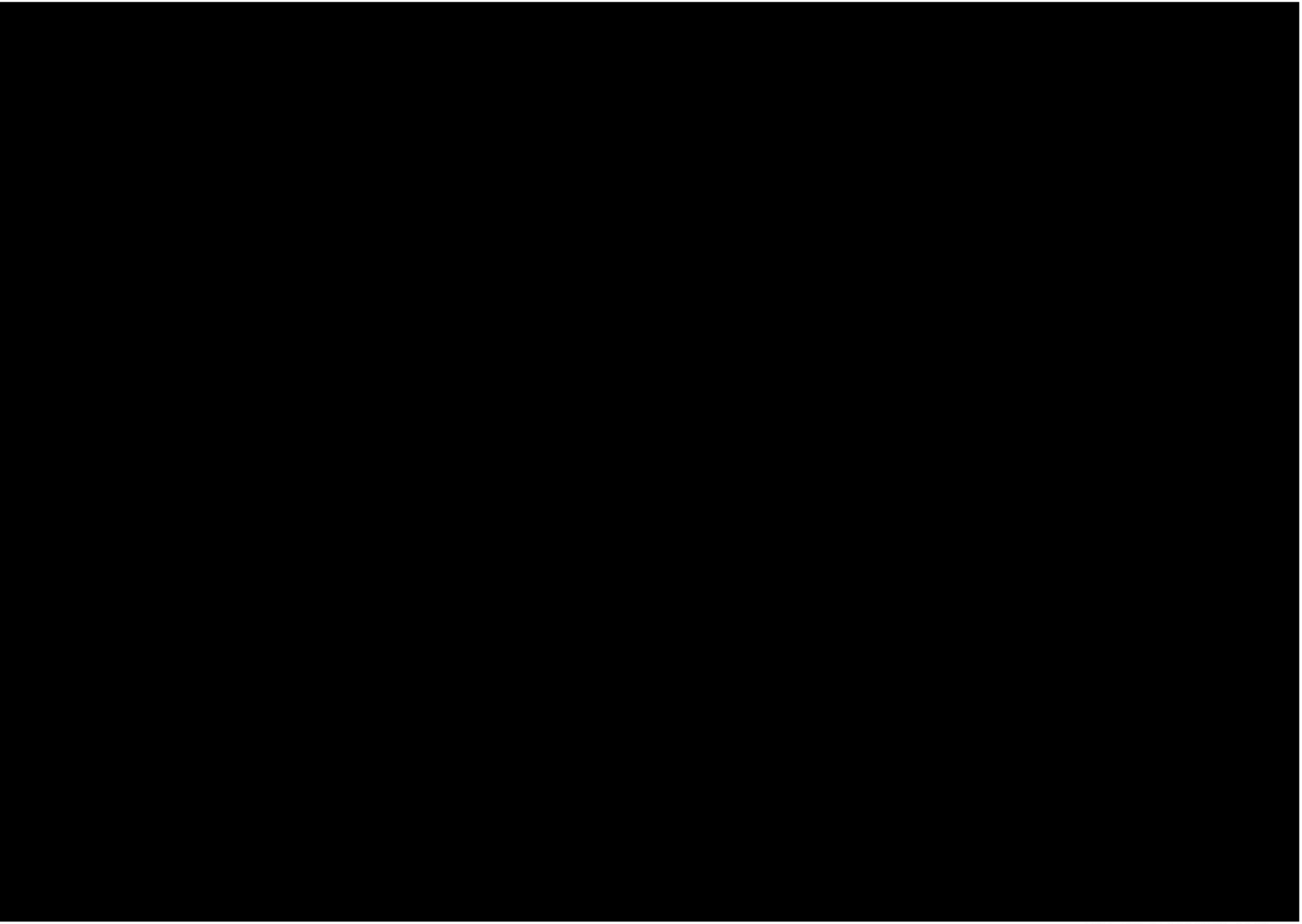
POL00401629



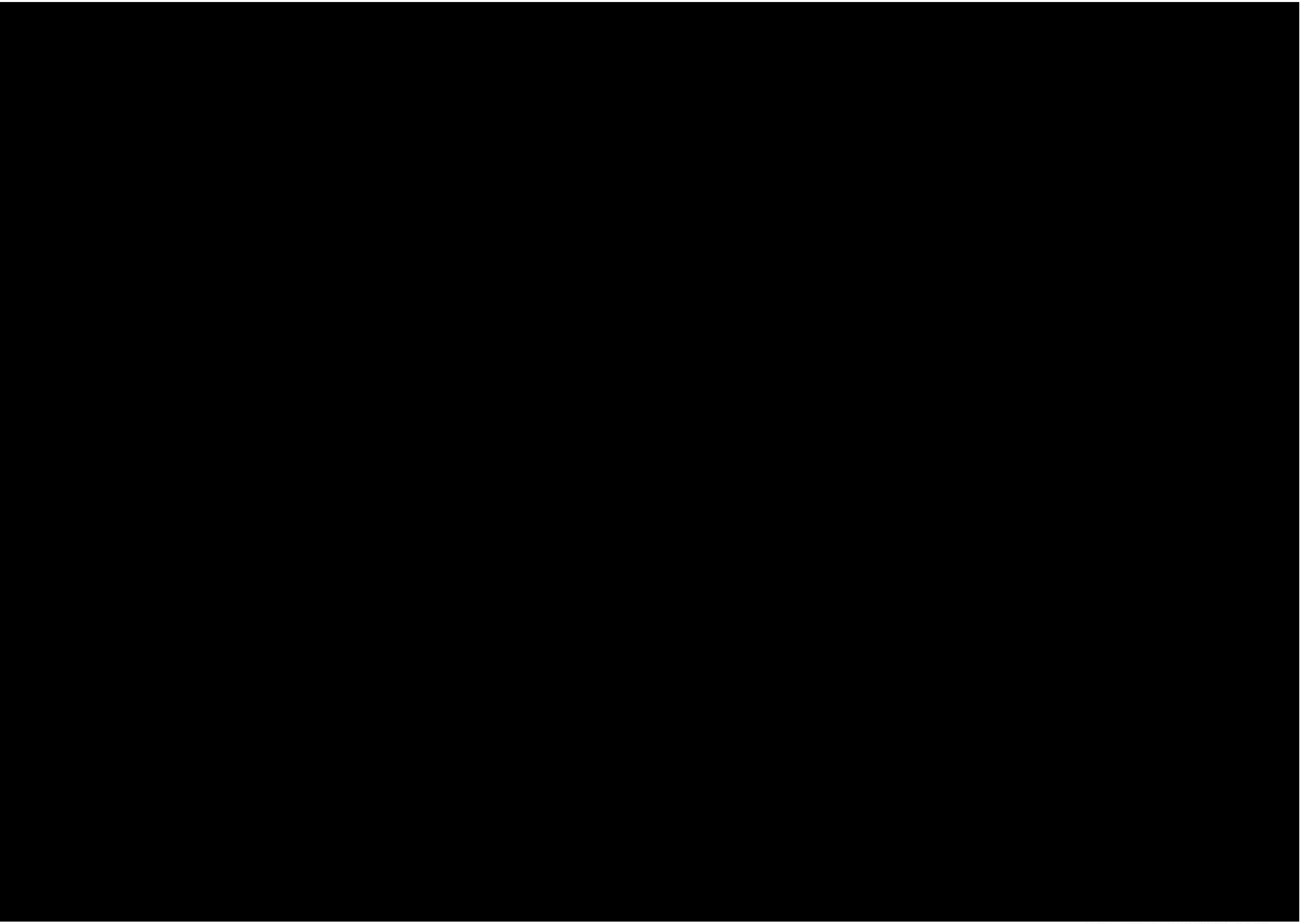
POL00401629



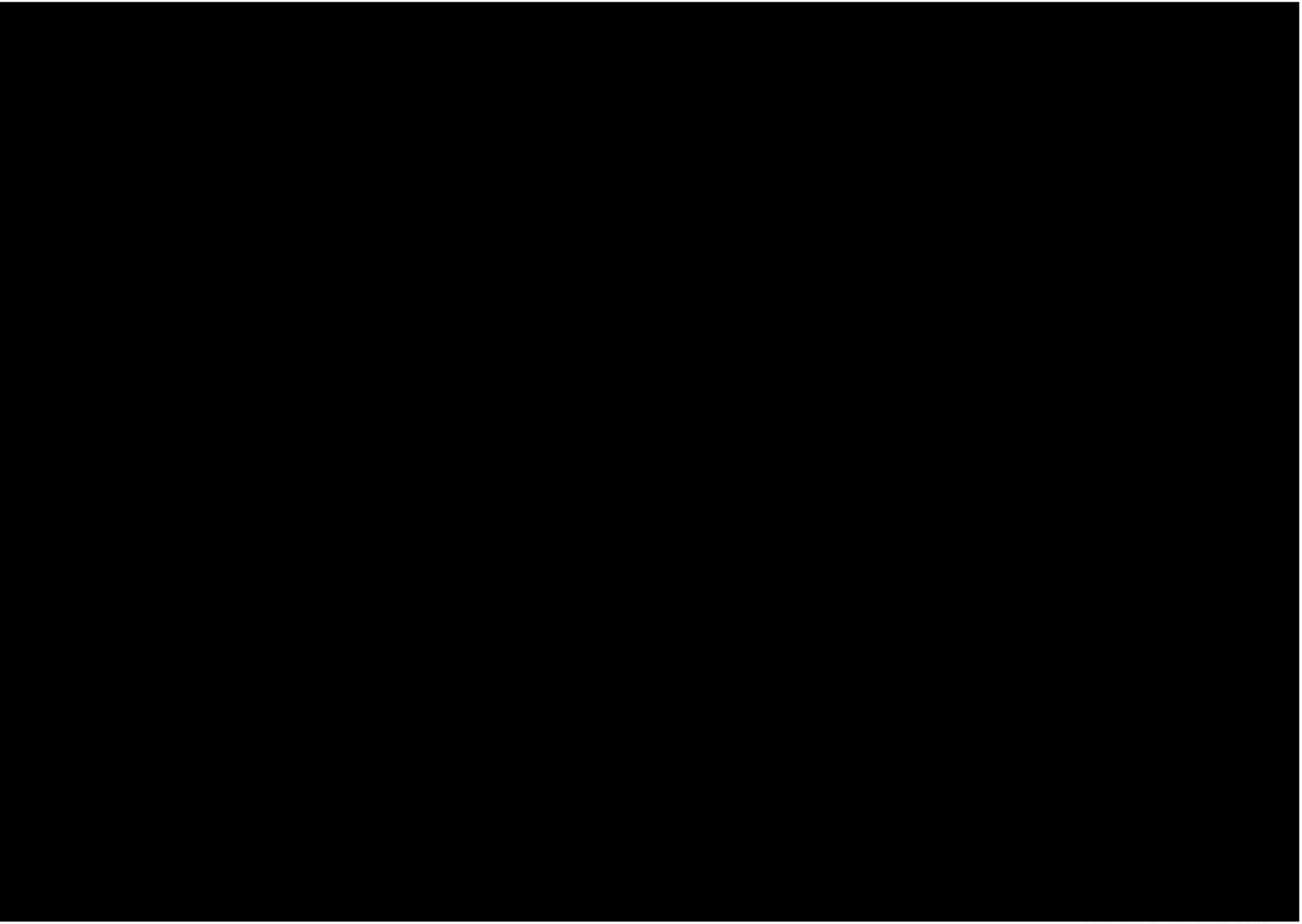
POL00401629



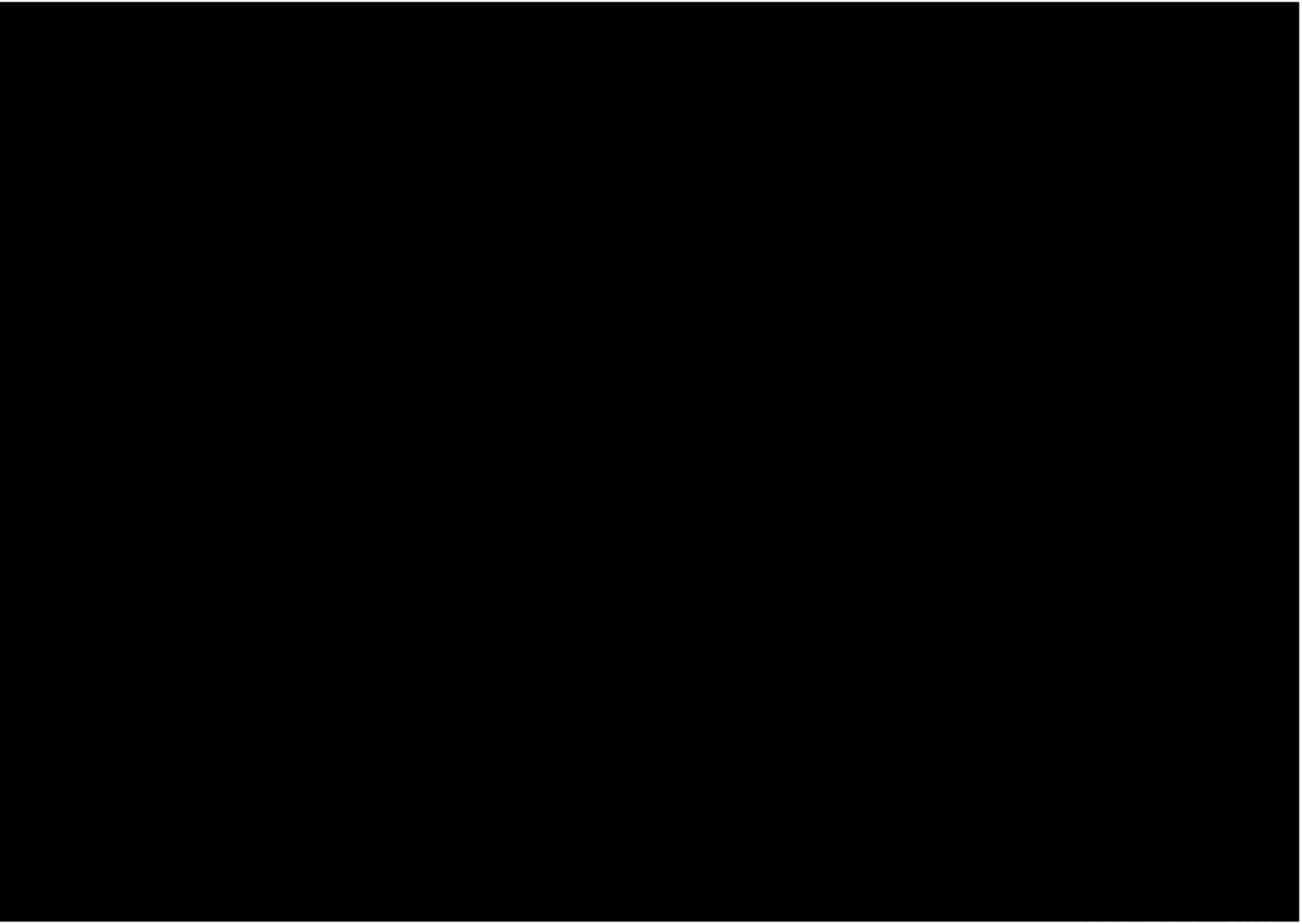
POL00401629



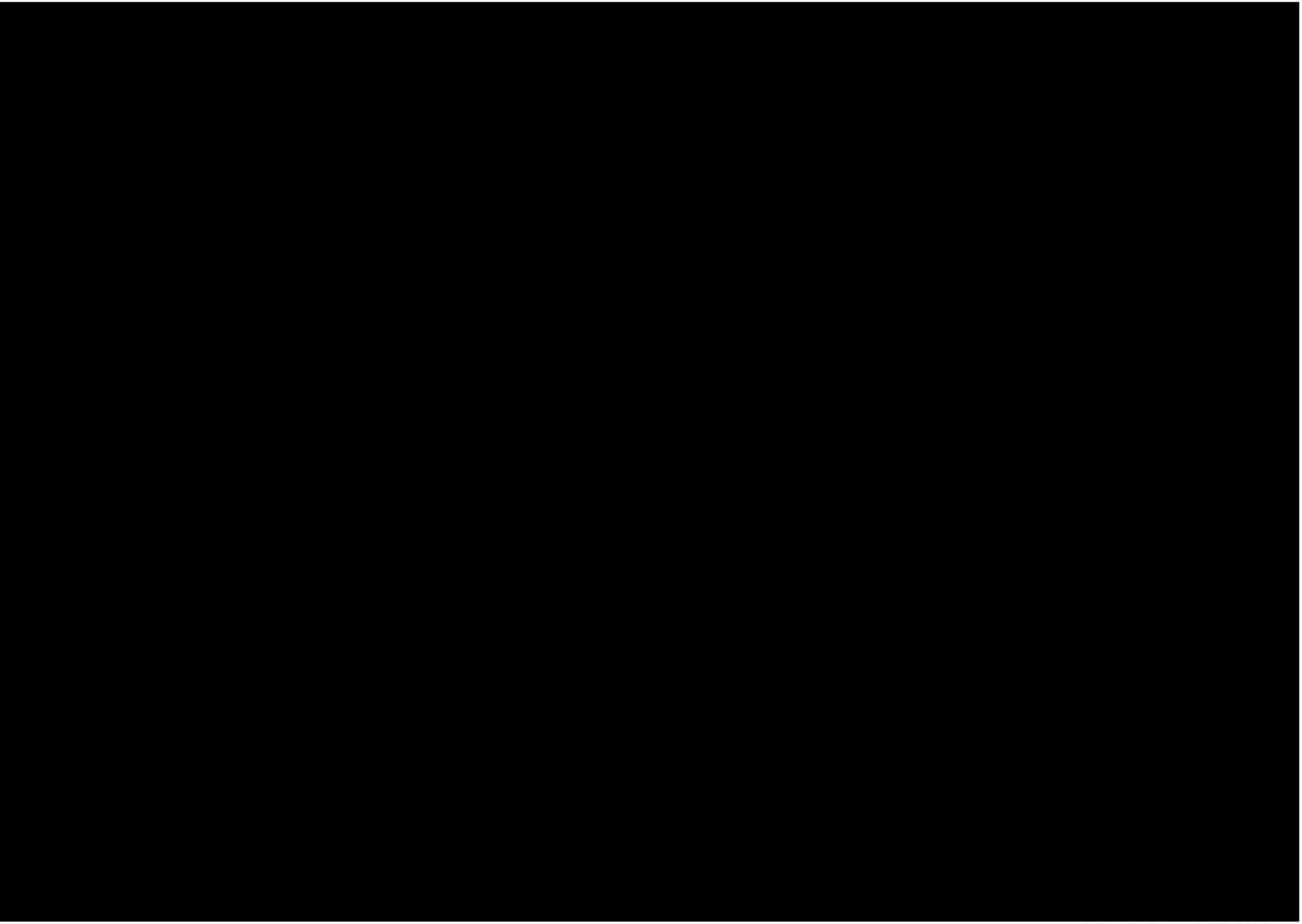
POL00401629



POL00401629



POL00401629



POL00401629

POST OFFICE LIMITED RCC REPORT

Title:	Progress update on the implementation of the Contract Management Framework	**Meeting Date:**	10 September 2020
Author:	Sarah Gray: Group Legal Director	**Sponsor:**	Ben Foat: Group General Counsel

Input Sought:

The RCC is asked to **note**:

- The final position achieved implementing the Contract Management Framework (the "CMF") with the most material contracts across the Post Office Group[1] (the "PO Group").
- The steps taken to ensure ongoing compliance with the CMF.

The RCC is asked to **approve** for consideration at the ARC on 22 September 2020:

- The final version of the CMF, which has been uploaded to the **Reading Room**.
- Mandating annual contract management training for all Contract Owners and Contract Managers, across the PO Group, via Success Factors.

Previous Governance Oversight

- Post Office ARC Meeting of 25 November 2019.
- Project Review Board of 14 January 2020.
- GE Tactical Meeting of 12 February 2020.
- Post Office RCC Meeting of 10 March 2020.
- Post Office ARC Meeting of 26 March 2020.
- Post Office RCC Meeting of 6 May 2020.
- Post Office ARC Meeting of 19 May 2020.

9

Executive Summary

1. The project implementing the CMF for the most material contracts across the PO Group 'completed' on 30 June 2020. All bar two of the 134 contracts identified by GE and GE-1 were located and uploaded onto Web3, with their obligations mapped[2].
2. Given Covid-19 and other commercial challenges, the Audit & Risk Committee ("ARC") in May approved all other non-material legacy contracts being 'remediated' (e.g. located, uploaded, mapped, contract manager assigned etc) via their respective natural 'lifecycles' as they are renewed, terminated and new contracts executed.
3. Against the original target of identifying, uploading and mapping obligations for 50 Material Contracts with funding of c£300k – the project spent c£100k, uploaded and mapped the

[1] Post Office Limited, Post Office Management Service, & Payzone Bill Payments Limited.

[2] We are working with the contract managers to obtain a signed version of the Kindred contract and locate the MediaZest contract (which is said to be in hard copy only).

Confidential

POL00401629

obligations for 132 Material Contracts[3], 43 Non Material Legacy Contracts[4], and identified (and received) benefits of c£440,000[5]. c£200k of 19/20 approved funding and c£600k of funding provisioned for in 20/21 (e.g. c£800k in total) has also been 'released back' to the business.

4. Resource and processes are agreed with CoSec, Legal and Procurement to ensure new contracts, as entered into across the PO Group, are compliant with the CMF.

Questions addressed

1. Did the project implementing the CMF for the most material contracts across the PO Group result in all Material Contracts being uploaded onto Web 3 with their obligations mapped?
2. What further steps have been taken to ensure compliance with the CMF going forward?

Report

1. At the meeting on 19 May 2020, the ARC approved the recommended approach whereby the project would:

   - seek to complete the upload and mapping of all remaining contracts identified by the GE and GE-1s as being material in terms of strategic and financial value by the end of June 2020 ("Material Contracts"); but

   - for those contracts not identified as being material by the GE or GE-1s ("Non Material Legacy Contracts") – compliance with the CMF would be achieved through their respective contractual 'lifecycles' e.g. as they are renewed, cease or new agreements are entered into.

2. It was noted that new contracts, as executed, were not yet under the CMF and that there would be ongoing annual costs of c£110k for licenses and resource costs in order to ensure the CMF is adhered to going forward. These costs will be funded by the project for 9 months, until July 2021, after which it will need to be funded as BAU.

3. The table below sets out the final position (on 30 June 2020) in respect of the Material Contracts:

Measurement	Original Target	Final Position (30 June 2020)
No. of Material Contracts identified	50	134/134
No. of confirmed latest versions of Material Contracts	All	132/134
No. of Material Contracts with Contract Managers	All	132/134
No. of Contract Managers on-boarded & trained via the LCG Academy	All (51)	51/51

[3] As defined below.
[4] As defined below.
[5] Through rebates due to Post Office as a result of Legal spend.

POL00401629

Measurement	Original Target	Final Position (30 June 2020)
No. of Material Contracts uploaded onto Web 3.0	50	132/134
No. of Material Contracts with obligations mapped	50	132/134
Rebates identified & realised	Not quantified	c£440,000
Spend vs £300k approved	£300,000	c£100,000

4. In addition to the numbers set out above, the project team also uploaded onto Web 3 and mapped the obligations for 43 Non Material Legacy Contracts.

5. There are two categories of contract which, post project, the PO Group needs to ensure there are processes, resource and funding in place for ongoing compliance with the CMF to be achieved:

   a. The remaining Non Material Legacy Contracts which were not identified by the GE and GE-1s as being material (in terms of financial or strategic value); of which there are estimated to be c1,500.
   b. New contracts the PO Group enters into ("New Contracts"), estimated at c30 per calendar month.

6. Although the ARC approved the c1,500 remaining Non Material Legacy Contracts being remediated over their natural lifecycle, the Source to Settle Programme ("S2SP") has a dependency on these contracts being uploaded onto Web3 in order to be able to realise its benefits[6]. As such, the S2SP project is onboarding temporary resource out of limited residual funds to identify, locate and upload the header level detail of as many as possible of these contracts (but not map the obligations). This approach will allow the S2SP to realise its benefits, with these contracts becoming fully compliant with the CMF as they expire or are renewed i.e. in line with the ARC's prior approval.

7. In respect of New Contracts:

   a. The final version of the CMF, including Supplier Relationship Management, has been agreed with Procurement and CoSec[7]. Processes are also being finalised with Procurement and CoSec to ensure these contracts are uploaded onto the Web3 platform, as they are executed.

   b. The Project will remain open for 9 months to fund the necessary resource to ensure:
      - Contract Owners and Contract Managers are identified, appointed and complete the internal CMF training delivered by the LCG Academy;
      - The Contract Manager is given a user license and completes training on Web 3;

9

[6] Timely, automated advance notification of expiring contracts, and access to the contract documentation will allow the Procurement team to effect compliant renewals and retendering processes particularly for small value contracts. More effective demand management processes prior to contract notice periods commencing will also reduce cost over time.
[7] Input has also been received from various other teams including IT, Post Office Insurance and Payzone Bill Payments Limited.

POL00401629

- The new contract is uploaded onto Web 3; and
- The obligation mapping is completed by the Contract Manager for the contract.

At the end of this period, funding or headcount will need to be provided in order to ensure ongoing compliance with the CMF.

c. **Templates**: The Legal team is populating Web3 with the updated template agreements from across all PO Group members. Contract Managers will be able to use these templates to negotiate contracts on the PO Group's standard terms and conditions. Supplier contracts will continue to be negotiated by the Procurement team with the support of the Contract Manager and other SME's.

d. Contract Managers '**Community of Practice'**: There is a 'Teams' site for all Contract Managers, which hosts key artefacts and training resources. IT vendor managers have created a community on Yammer that Contract Managers will be able to use to learn from each other, share their experiences, ask questions and support each other.

e. **Success Factors Training**: Every employee across the PO Group should be:
   - aware of the CMF;
   - directed to the right resources;
   - aware of the procedures and controls implemented.

   To ensure ongoing compliance and awareness the ARC is asked to give approval for the development and deployment of short annual mandatory training on the CMF and Public Contract Regulations for all Contract Owners and Contract Managers, across the PO Group, via Success Factors. The Learning and Development Team has been engaged and are supportive, pending approval from the RCC and ARC.

Confidential

POL00401629

POST OFFICE LIMITED RCC REPORT

Title:	Update on Postmaster Accounts	**Meeting Date:**	10 September 2020
Author:	Tim Perkins	**Sponsor:**	Alisdair Cameron

Input Sought:

The RCC is asked to **note**:

- The update on Postmaster customer accounts following a request at ARC in July 2020.

The RCC is asked to **approve** the recommended approach:

- Whereby, following the review of Stamps processes, KPMG are instructed to explore whether there are other identified product processes that could give rise to similar issues as those identified with Stamps.

Previous Governance Oversight

- None

Executive Summary

1. The Audit and Risk Committee asked, following KPMG's reviews of the current operation of suspense accounts and stamps processes, for an overview of the processes deployed to inform Postmasters of balances on their customer accounts and for consideration to be given to reviewing other product processes in line with the review on stamps.
2. Postmasters with a balance on their account are sent a letter (or letters) on a trading period basis encouraging them to make contact with Post Office to discuss the balance. The letters sent by Post Office changed significantly following the Common Issues Judgment and Post Office also stopped automatically deducting balances from remuneration when no contact was made by a Postmaster. The revised processes and letters have been independently reviewed and approved by Norton Rose Fulbright as reflecting the requirements of the Common Issues Judgment.
3. Post Office has seen balances posted to Postmaster customer accounts fall over the last 20 months, with decreases in both the volume and value of balances posted. This reduction in balances posted to customer accounts is in line with a reduction in the level of losses in branches.
4. However, the overall balance on Postmaster customer accounts has risen over the same time period, primarily as a result of reduced recovery after stopping automatic deduction from remuneration for Postmasters after the Common Issues Judgment.
5. Post Office is currently reviewing its Loss Recovery policies and processes and completing a review of its aged debt and these reviews will conclude in Q3 2020.
6. Following the review of stamp related processes, it is recommended that the RCC approve instructing KPMG, at a cost of c£106k, to perform a similar piece of assurance work across Post Office's wider product portfolio, in respect of both current and historic processes.

10

Confidential

POL00401629

Questions addressed

1. What processes are in place to inform Postmasters of balances on their customer account?
2. What trends are prevalent or emerging in Postmaster customer accounts?
3. What further work could KPMG perform to assess whether any other product processes could have given rise to similar issues to those identified with stamps? How much would this cost? What are the limitations and risks?

Report

Informing Postmasters of balances on Postmaster customer accounts

1. Every Postmaster has a customer account for each branch that they operate. These are the accounts used to hold balances that are settled centrally at the end of a trading period.
2. Branches are expected to complete trading period accounting 12 times a year on a 5 week, 4 week, 4 week schedule at the end of each trading period. Branches are organised into 4 balancing groups (A-D) – this means that in 12 of any 13 weeks, there will be a group of branches scheduled to complete their trading period accounting and balances will be posted to Postmaster customer accounts.
3. On the Monday following the scheduled branch balancing date, a letter is sent to the Postmaster by the Loss Recovery team informing them of any balance on their account. This letter is appended to this paper as **Appendix A**. If, by the following Tuesday, the Postmaster has not contacted the Loss Recovery team to discuss the balance on their account, a second letter is sent by way of follow up. This letter is appended to this paper as **Appendix B**. A copy of a statement of their customer account is enclosed with both letters sent to the Postmaster. A redacted version is appended to this paper as **Appendix C**.
4. The letters sent to Postmasters regarding balances on their accounts have been changed significantly since the Common Issues Judgment. It is also worth noting that Post Office used to automatically deduct monies owed by a Postmaster from their remuneration when there was no response to letters. This practice stopped immediately after the Common Issues Judgement.
5. The revised processes and letters have been independently reviewed and approved by Norton Rose Fulbright as reflecting the requirements of the Common Issues Judgment.
6. Post Office is currently completing a thorough review of its Loss Recovery policies and processes and is considering other opportunities, such as the use of Branch Hub, to allow Postmasters to monitor the balances on their customer account(s). The review will conclude in Q3 2020-21.

Postmaster current accounts – analysis and trends

7. The balances settled centrally by branches at the end of each trading period have been falling in the last 20 months. Apart from in TP04 2020, the year on year balances settled centrally by branches have fallen year on year in each trading period of the last 20.
8. The reduction in balances settled centrally is driven by a reduction in both the volume of branches settling balances centrally and the average value being settled centrally.
9. This pattern aligns with the reduction in the total level of declared losses across the network. **Appendix D** shows the reduction in both declared losses and balances settled centrally over the past 20 months.
10. The reduction in declared losses is driven by an increase in the monitoring of branches, an increase in the support provided to branches and through more frequent earlier intervention

POL00401629

for branches that are having operational issues. The focus of the Loss Prevention team has been on ensuring that network trading compliance has improved (completion of cash declarations, trading period accounting and stock remittances), increasing contact levels with branches to offer enhanced support (through SPEAR visits and calls) and offering enhanced reactive support for balancing issues through Tier 2 Branch Support.

11. The table below shows the average number of branches settling balances centrally per week and the average value of the balances settled centrally:

Trading Period	Average number of branches settling a balance centrally per week	Average value of balances settled centrally
TP10 2018	48	£135,828
TP11 2018	68	£275,773
TP12 2018	56	£189,901
TP01 2019	61	£134,023
TP02 2019	68	£225,762
TP03 2019	63	£195,367
TP04 2019	52	£134,713
TP05 2019	75	£173,576
TP06 2019	65	£194,157
TP07 2019	52	£148,891
TP08 2019	64	£142,273
TP09 2019	69	£153,497
TP10 2019	60	£128,766
TP11 2019	65	£141,245
TP12 2019	64	£138,846
TP01 2020	37	£97,467
TP02 2020	52	£85,907
TP03 2020	43	£111,472
TP04 2020	41	£144,284
TP05 2020	58	£106,577

12. Whilst the value being settled to Postmaster customer accounts on an ongoing basis has fallen, the total value held in Postmaster customer accounts has increased over the same period. This is due to lower levels of recovery primarily as a result of Post Office no longer automatically deducting balances held in Postmaster customer accounts from remuneration payments.
13. There is currently £4.1m of debt held on Postmaster customer accounts for current Postmasters and there is £13.3m of debt held on Postmaster customer accounts for former Postmasters.
14. The £13.3m debt for former Postmasters has been fully provided for in Post Office's accounts and has a number of aged cases within it. The £4.1m of debt for current Postmasters also contains a number of aged cases with all debt over 60 days in age fully provided for in Post Office's accounts.
15. The review of Post Office's Loss Recovery processes will also consider, in conjunction with the Historical Matters programme, how to manage and resolve aged debt in the Postmaster customer accounts.

10

Assessment of further product processes following the Stamps review

16. A recent review of Post Office's stamps processes found limited evidence of detriment suffered by Postmasters as a result of weaknesses in Post Office's stamps processes and controls. These findings have been reported to the ARC and Board and Post Office is now establishing a Scheme to provide redress to Postmasters who may have suffered detriment.
17. Stamps are one product set from a wide portfolio of products sold by Post Office and transacted through the Horizon system.

POL00401629

18. The stamps review commenced as a result of internal identification of potential risk in the processes.
19. Whilst there have been no further products or product sets identified internally that are deemed to have similar risks to stamps, Post Office is looking to adopt a holistic approach by undertaking a high level review of its product portfolio in order to identify key risk areas and any products with specific process issues that may have the potential to cause product-related branch discrepancies and where Postmasters may have suffered detriment as a result of these or as a result of the monthly discrepancy settlement process.
20. This review will include, as a minimum, processes for ATMs, Camelot (lottery and scratchcards), Paystation, Moneygram, Postal Orders, Foreign Exchange and Traveller's Cheques. The review will consider current and historical processes, where historical processes are known.
21. It is recommended that the RCC approve instructing KPMG to complete this review. KPMG has provided a cost estimate of c£106k to complete this work.
22. The RCC should note that any documentation which is produced and findings made, may be disclosable as part of Post Office's ongoing disclosure obligations to those it has prosecuted historically and as part of any future claims made against Post Office as a result of historical practices, in both a civil and criminal context and in the context of any future investigation or inquiry.

Confidential

POL00401629

Appendix A – Discrepancy 1 letter

Branch Code: XXXXXX
Customer Account: XXXXXXX

Dear XXXXXXXXXX,

Discrepancy identified for XXXXbranch nameXXXXXXXXXXX Post Office® branch

We're writing about the discrepancy of £xxxx which has been settled centrally in branch at the end of the trading period. Please find enclosed a statement showing the total amount of the discrepancy and a breakdown of how the total has been reached.

We would like you to get in touch with us to discuss this further so you can decide whether to accept the discrepancy by paying the balance, or dispute the discrepancy.

Accepting the discrepancy

If you accept the discrepancy, please can you contact my team on GRO or agents.accounting.team GRO to discuss the appropriate course of action:

- arranging payment of the amount;
- arranging a deduction from your remuneration/fees to cover the amount;
- arranging an instalment plan; or
- investigating the discrepancy further.

Disputing a Discrepancy

If you have not already disputed the discrepancy and would like to do so, please contact us to confirm this and provide any information you may have as to how or why you consider that the discrepancy may have arisen. Details of how to do this for each type of discrepancy are set out below.

a) Disputing a Branch Discrepancy

If the entry on your statement relates to a Branch Discrepancy, and you wish to dispute this, please call the Branch Support Centre (NBSC) on GRO.

b) Disputing a Transaction Correction

If the entry on your statement relates to a Transaction Correction, and you wish to dispute this, please contact the Transaction Corrections Disputes Team on GRO or call us on GRO.

Please respond to this request by making contact with us using the appropriate details above within the next seven days.

Yours sincerely,

Michelle Stevens

Loss Recovery Manager

Enclosures:

Statement

Confidential

POL00401629

Appendix B – Discrepancy 2 letter

Branch Code: XXXXXX
Customer Account: XXXXXXX

Dear XXXXXXXXXX,

Discrepancy identified of £XXX for XXXXbranch nameXXX Post Office® branch

We've previously written to you about the above discrepancy of £XXXX which was settled centrally in branch at the end of the trading period. In our letter we provided you with a statement and breakdown of how the total has been reached and asked you to contact us to discuss this further.

Accepting the discrepancy

As set out in our previous letter to you, if you accept the discrepancy, please can you contact my team on GRO or agents.accounting.team GRO to discuss the appropriate course of action:

- arranging payment of the amount;
- arranging a deduction from your remuneration/fees to cover the amount;
- arranging an instalment plan; or
- investigating the discrepancy further.

Disputing a Discrepancy

If you have not already disputed the discrepancy and would like to do so, please contact us to confirm this and provide any information you may have as to how or why you consider that the discrepancy may have arisen. Details of how to do this for each type of discrepancy are set out below.

a) Disputing a Branch Discrepancy

If the entry on your statement relates to a Branch Discrepancy, and you wish to dispute this, please call the Branch Support Centre (NBSC) on GRO.

b) Disputing a Transaction Correction

If the entry on your statement relates to a Transaction Correction, and you wish to dispute this, please contact the Transaction Corrections Disputes Team on GRO or call us on GRO.

Please can you contact us to discuss in the next seven days.

Yours sincerely,

Michelle Stevens

Loss Recovery Manager

Confidential

POL00401629

Appendix C – Example statement

Branch Code:	Customer Account:	Customer Name:
XXXXXX	XXXXXXX	XXXXXXXXXXX

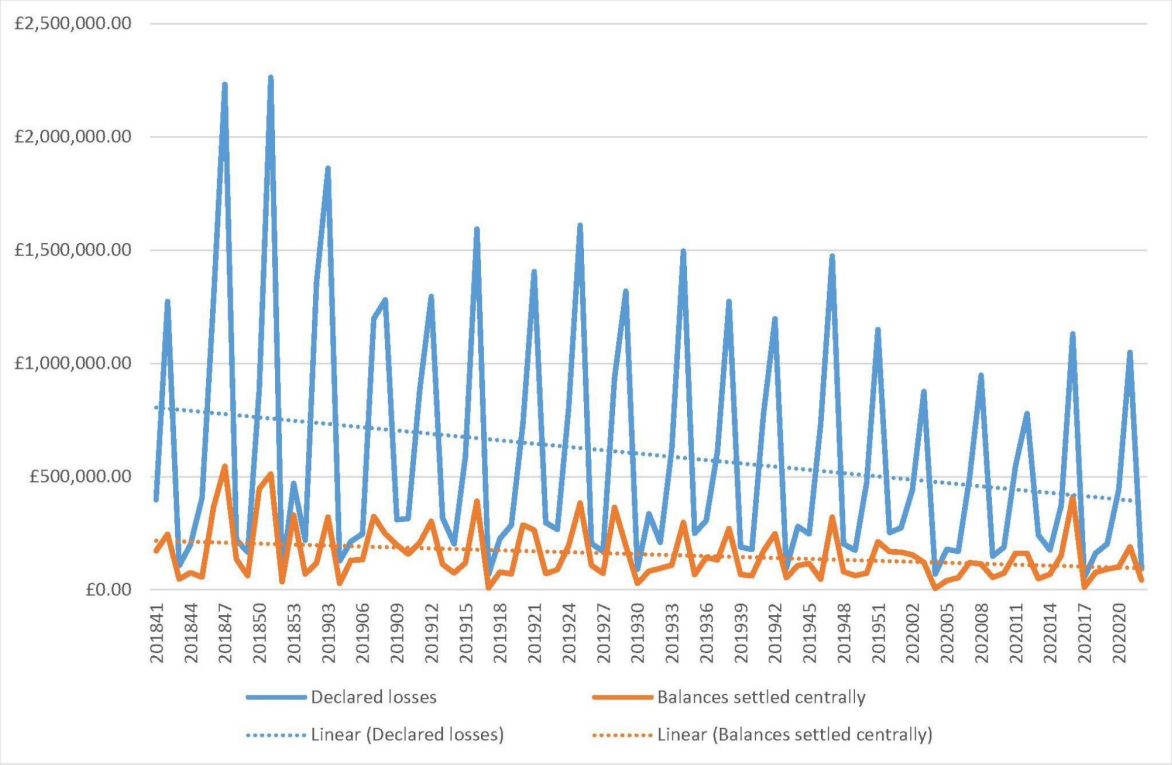
Please find below the statement of account from the period 01 Oct 2019 to 25 Oct 2019

Document number	Transaction Detail	Document Date	Amount	Currency
Outstanding Discrepancies				
6200000010	Transaction Correction	01.10.2019	100.00	GBP
6200000011	Branch Discrepancy	03.10.2019	200.00	GBP
Total			**300.00**	**GBP**
New Discrepancies				
6200000012	Transaction Correction	07.10.2019	300.00	GBP
6200000013	Transaction Correction	05.10.2019	400.00	GBP
Total			**700.00**	**GBP**
Previously Agreed Discrepancies				
6200000014	Final Account	08.10.2019	1,000.00	GBP
Total			**1,000.00**	**GBP**
Disputed Discrepancies				
6200000015	Branch Discrepancy	02.10.2019	760.00	GBP
Total			**760.00**	**GBP**
Settlement Total			**2,760.00**	**GBP**

Confidential

POL00401629

Appendix D – Trends for declared losses and balances settled centrally



10

Confidential

POL00401629

Post Office Limited - Risk and Compliance Committee-10/09/20

POST OFFICE

Success Factors @ POL

Deep Dive & Forward Planning

Sept 2020

POL00401629

Success Factors – Audit Update

This paper demonstrates the progress made in addressing the concerns raised about the Success Factors HR platform and shows how we propose to drive greater value from the system in line with the development of the HR TOM.

It also considers whether a 'reconfigured' Success Factors should play a longer term key role in delivering the new HR Service Delivery Model.

ARC are requested to review and approve the stated recommendations for the future of Success Factors at POL.

A summary version of this paper is in the

successfactors™ An SAP Company

- Background and Context
- Success Factors 'in use' at POL
- Audit Questions Response
- Success Factors Activity 2020
- Considerations & Risks
- Recommendation
- Appendix

POL00401629

Background & Context

- Success Factors is currently one of the leading HRIS platforms used by over 6850 organisations and over 125m users worldwide. It offers modules to support the management of people data and the processing of employee activity throughout the employee journey providing automation and mobile access to key HR services. Like most comparable products on the market, Success Factors can be heavily customised, however, it operates at an optimal level, when it supports consistent data sets and common, simple processes

- Success Factors HR suite was first purchased by POL as part of a settlement of a SAP Audit in 2016, which found POL to be significantly under licensed on SAP products. The agreement removed the liabilities on the licence issue and offered a full Cloud solution to deliver key HR services via the Success Factors platform (including payroll and HR data) - this formed a key pillar of the 2016 HR Transformation Programme. The agreement meant that the Success Factors (SF) purchase was not subject to the full procurement process

- The original implementation of 'Success Factors' at POL was not without challenge. The design was not fully scoped and the project failed to address the complex processes that are in play across POL HR, attempting instead to build workarounds for the anomalies and lack of consistency in the contractual agreements with our people. In short, the project tried to overlay complex and inconsistent ways of working onto a new technology platform that offered the greatest benefits when paired with simplicity and commonality. This resulted in a mix of an underutilised system and manual workarounds that eliminated efficiency gains

- Following delays and a substantial increase in budget, an external audit (by PWC) recommended a positive go-live decision and SF payroll was launched in January 2018. Following the payroll launch an internal audit revealed further issues with the implementation. Other modules introduced included Recruitment, Onboarding, Performance & Goals and Learning. Whilst these modules have introduced benefits and value to the organisation, it is recognised that the configuration of these modules at the time was also not optimal

- Changes in HR Leadership, organisation strategy and the Covid 19 situation have interrupted and slowed progression to resolve the issues raised with Success Factors. However, since the start of 2020, concrete actions have been taken to identify and prioritise activity that will drive and maximise the value we obtain from the system. This includes addressing the complexity of HR as we develop the HR TOM

POL00401629

Success Factors IS working at the Post Office

3741*
People were paid by Success Factors in July '20
* Note this is heads and NOT FTE which will be a smaller number

25%
reduction
in payroll errors since the introduction of Success Factors
(and these are now cleared **before** live payroll)

309
employees have been recruited through Success Factors in the last year
(Aug '19-Aug'20)

There are
1312
active performance review forms in the system for the current year*
* Only grades 2b and above currently participate in the online process

In July '20 the System received on average
500
log ins per day
(with over 1000 people accessing on 22/07)

Over
400
Learning resources are available within Success Factors

11,758
compliance training courses have been completed via Success Factors

over
46,500
individual Items of Learning have been accessed / completed in the last year

Adoption of Success Factors Learning has increased by
217%
in the last year

System availability in the last year was
99.9%
Services continued to be accessible throughout the Covid pandemic lockdown

During the extended lockdown period we were able to support employees remotely via Success Factors – launching a 'wellbeing' learning collection of resources, TED talks and 'book club' style discussions, designed to support employees navigate the challenges of this unique time





POL00401629

Success Factors IS already adding value at the Post Office

PAYROLL

- Ability to run frequent 'test' payruns has reduced errors and eliminated system downtime during investigations
- Exceptions reporting is more advanced and efficient. For example, the test run highlights risks with employees who are outside regulatory requirements (eg. Minimum wage)
- Payslip and P60 production are automated and available online, reducing costs and requests for duplicates
- Other processes such as payment for court orders, tax code changes and student loan deductions are now automated and have removed manual processes - prone to input error

PERFORMANCE & PENSIONS

- Performance process is run online for all grade 2b and above employees. Success Factors has improved transparency and consistency in the process and created more accurate reporting.
- Nearly 90% of eligible employees have objectives recorded in the system
- The online performance process has eliminated a number of manual spreadsheet conciliation processes
- The first round of Pensions Auto-Enrolment has been completed using SF

LEARNING

- The Learning Module is available to over 3400 'learners'
- 98% of learners find the online learning 'easy to navigate'
- Moving compliance training onto Success Factors has improved compliance reporting and has reduced the average time window taken in which to complete the training from 23 days to just 4 days
- Aside from online learning, the system also manages administration for 432 facilitated sessions – over the last 12 months it has managed over 2800 course bookings

RECRUITMENT

- Process now sits in one system rather than two – improving the user experience
- All user data now sits on one page rather than across multiple tabs, saving time to review details
- There are fewer errors with new entrants personal details as they are entered by the individual directly
- The Onboarding module is currently awaiting an upgrade to ONB2 in order to automate more activity

POST OFFICE

5

POL00401629

The BIG Questions

Is Success Factors fit for purpose – What are the current risks we face with the product?

Success Factors is without doubt, one of the leading HRIS platforms used globally. It may not be perfect, but it should be noted that, on average, at POL it has over **500 log ins per day** and delivers many essential HR services including **Payroll, Onboarding, Recruitment, Performance and Learning**. It has also introduced employee 'self serve' processes which will be key to future HRSC development.

The success of any HRIS is wholly dependent on the quality of the design and build and it is clear that the original configuration was not optimal and whilst the required functionality sits within the system it is often not being fully utilised. The complexities of the business operations have resulted in a complicated build that is difficult to maintain and update and is supported by many manual workarounds.

The main risks that the organisation faces with SF is that we continue to try and configure and 'fix' the system issues without addressing the business processes that are driving them. Simplifying processes, aligning policy where possible and removing complexity will address the risk and reduce, rework, duplication of activity, maintenance and development costs. In some areas of the business, SF has also lost credibility, which could be regained through delivery of improved 'user focussed', simplified processes.

Are there alternative products or upgrades to be considered?

There are many alternative products available providing a connected suite of HR service modules (Workday being the main competitor - but this also has limitations). Another option is sourcing independent systems to meet specific service requirements (eg. learning, payroll, performance management). These would require significant investment and integration to implement, run and connect and usually result in a more complex system landscape.

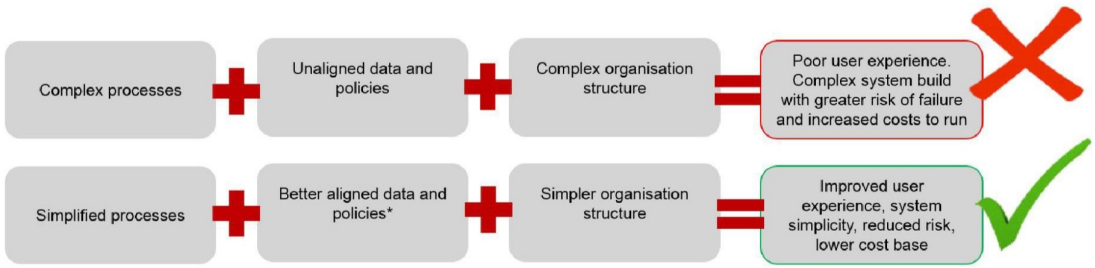
It should be noted that any new implementation would likely end in the same result unless processes and ways of working are significantly simplified and there is an acknowledgement that the system and accompanying processes have to be built for the majority / future state - not to support small legacy populations with specific needs who may not play a part in the longer term strategy.

POL00401629

The BIG Questions

If Success Factors is retained, how can we maximise the return on investment? (for example, in staff training, capability building to reduce errors and adopting and embedding new ways of working)

- Simplification of core processes, simplification of org structures through POM and ongoing work to align T&Cs and employment contracts is underway. Quick wins from a Deloitte review from March 2020 are being applied as a part of the process improvement stream that is inflight. Together, these will deliver efficiencies and system improvements that will add real value by removing complexity, duplication, rework, manual work arounds etc.
- As a part of the continued development of the HRSC we will naturally look to harness the Success Factors technology, where possible to provide increased automation, self service and mobile access. This will reduce the business reliance on outdated, laborious HRSC processes and will lead to a more efficient, leaner HR function
- We will also looking to update Role Based Permissions (RPB) to ensure that HR administrators have wider access to complete HR activity workflows in the system rather than pass small activities from team to team (with different permissions) to administer. This creates further process efficiencies, increases process control and reduces risk from handoffs
- Internal PR and training around system functionality will be improved to create new excitement and demonstrate clear benefits



* There will never be complete alignment and will always be exceptions, but systems should be built around the majority and not overly customised to meet niche needs and anomalies – which drive complexity, cost and risk

Simple system efficiencies adding value:

Currently 1FTE spends several hours each day running reports and contacting managers to inform them that they need to follow up ongoing absence.

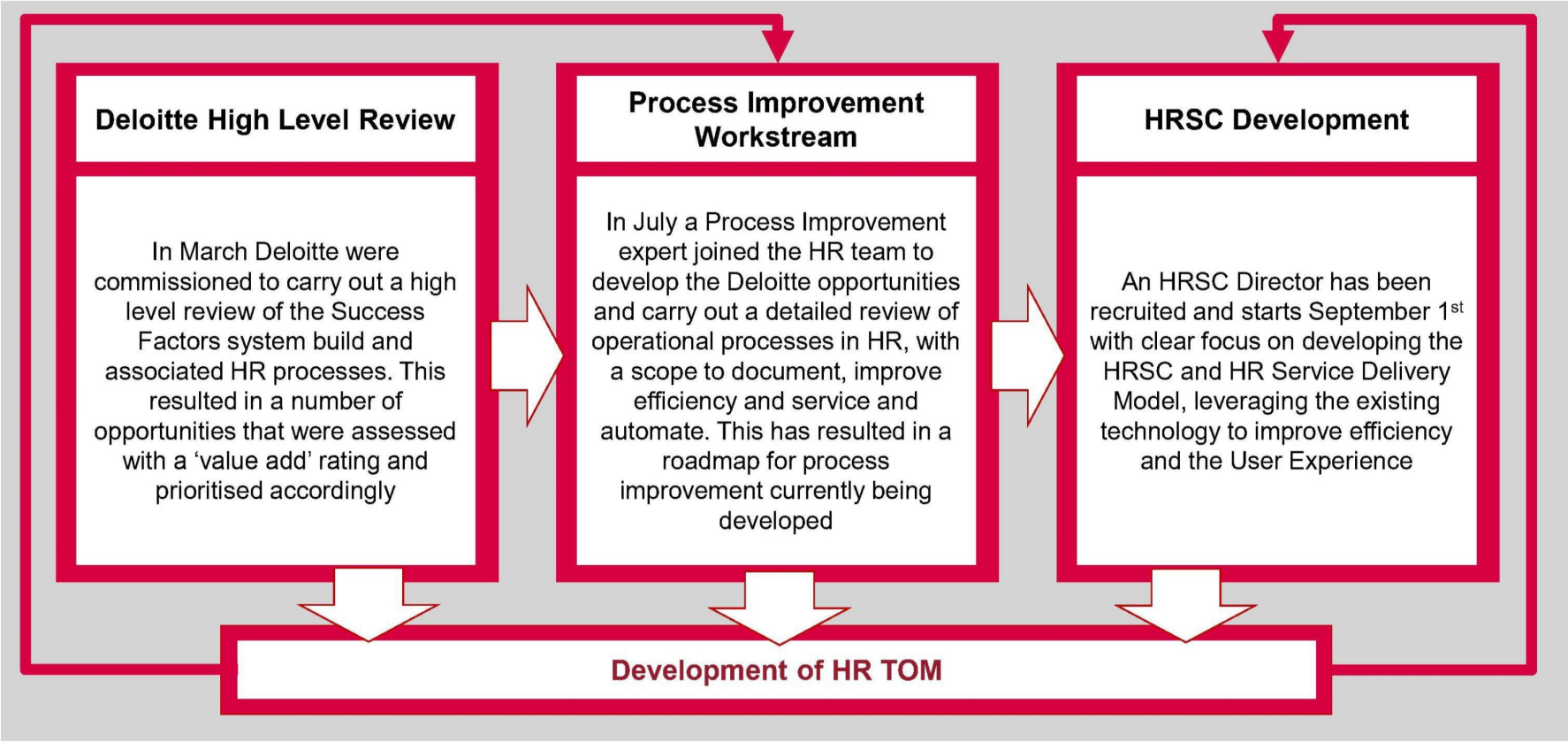
An automated flag is being added to the system that will send a reminder to Managers automatically – saving significant effort every day

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Success Factors in 2020

Three key activities have been instigated in 2020 to drive efficiency across HR, leverage SF functionality and support the HR TOM:



Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Summary of Activity Findings

- The **Deloitte high level review** revealed 51 opportunities that would improve the integrity of the system and improve functionality, connectivity, governance and reporting (See appendix for full list)
- Of the 51 opportunities, 21 'quick wins' were identified which could be delivered relatively easily with minimal cost.
- 22 opportunities were identified as 'Priority' based on value add. These have been 'combined' and worked up into 14 'prioritised opportunities'

- The **Process Improvement workstream** is developing these opportunities at a more detailed level and is looking more broadly at processes across the HRSC.
  - Including the Deloitte activity, 176 process improvement opportunities have been identified that could result in an estimated 32% time saving (currently at Prove Plan)
  - Initial focus on developing 2 key processes is estimated to save 1FTE
  - As a part of the work all processes are being fully documented
  - Support, Training and a control forum are being worked into the new HRSC development work
  - An additional opportunity for a HRSC service management tool integrated with SF has been identified as another way to streamline HRSC ways of working and improve the customer experience but would require additional funding

Deloitte Review – Breakdown of opportunities by HR functional area					
Advice Centre, Recruitment & Administration	**HR Systems & MI**	**HRSC**	**Pay Processing**	**Change & Integration**	**Rewards & Pension**
14	**16**	**5**	**10**	**5**	**1**

POL00401629

Deloitte Review - Potential benefits identified for shortlisted opportunities in People

The benefits of transformation and automation are broad and impact multiple areas of the business. Below is an overview of the potential benefits to be achieved if the prioritised People Opportunities are carried out

EMPLOYEE EXPERIENCE

- ***93%*** *of prioritised People opportunities have been identified to have a positive impact on employee experience*

EXTERNAL CUSTOMER SATISFACTION

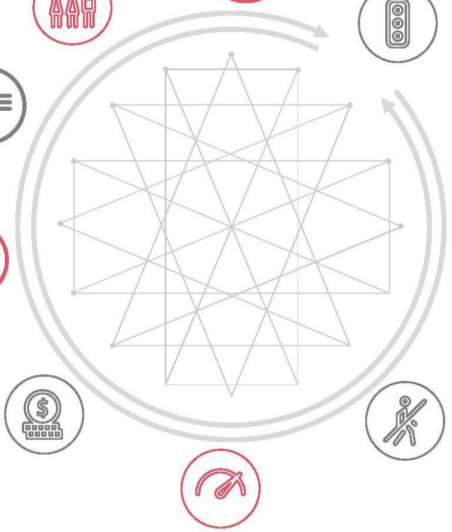
- ***71%*** *of prioritised People opportunities have been identified to have a positive impact on external customer satisfaction*

JOB SATISFACTION OF CURRENT TEAM

- ***100%*** *of prioritised People opportunities have been identified to have a positive impact on job satisfaction*
- *Having better processes, automated where relevant and improved use of existing systems will allow teams to focus on value add activities, increasing overall satisfaction*

OTHER COST SAVINGS

- *Shift of knowledge and activities from Support Vendor to POL would reduce current costs of the support contract*
- *As a result of higher efficiency and less manual rework, there will be further FTE savings. These will become clear as opportunities are realised e.g. End to End Payroll Review*



MAXIMISE EXISTING TOOLS

- ***79%*** *of prioritised People opportunities have been identified to help maximise / optimise use of existing POL tools and systems*

IMPROVE DATA QUALITY AND ANALYTICS

- ***71%*** *of prioritised People opportunities have been identified to have a positive impact on data quality and improve analytics and reporting capabilities*
- *Improved data quality at the source of entry significantly reduces (re)work activities within the HRSC*

KPI / REGULATION COMPLIANCE

- ***71%*** *of prioritised People opportunities have been identified to help increase compliance and meet internal and external KPIs*
- *Improved data quality and better data oversight / audit trails produces invaluable data which can be analysed to provide visibility and insight into the business processes*

INCUR FINANCIAL OR REGULATORY PENALTIES

- ***43%*** *of prioritised People opportunities have been identified to help reduce risk of penalties or overpayments*
- *Improving Payroll Processes and validation checks in the run phase*

IMPROVE DATA QUALITY, ACCURACY AND REDUCE MANUAL REWORK

- ***86%*** *of prioritised People opportunities have been identified to reduce manual rework and improve accuracy*
- *Removing or reducing the manual effort in processes (through systems optimisation or automation) result in time saved and faster turnaround times within the HRSC*

POL00401629

Deloitte Review Observations & HR Response

Deloitte Observations - Summary

- Employee Experience is not embedded in current SuccessFactors Design, limiting end user capability for optimal use
- Lack of internal capabilities causing high dependency on vendor support to deliver urgent system changes
- Limited flexibility in the Service Centre to deliver bespoke changes and value for money
- Limited ability to effectively and quickly produce reporting
- People Analytics are not pro-actively delivered with a commercially minded approach
- Lack of clear roles and responsibilities in HRSC
- Limited 'Self-Serve' model embedded within current HR Processes
- GDPR limiting the current Role Based Permission set up within SuccessFactors
- Inability to measure performance or where improvements are required
- Undefined and undocumented processes lead to duplication and/or error

New HRSC Director to start on September 1st – will be targeted on developing the HRSC Service Delivery Model with a view to harnessing the capability of SF, increasing automation and self service (and improving employee experience)

The 21 Quick Win Opportunities are being integrated into the current Process Improvement Workstream (which is also documenting all processes and looking at Role Based Permission dependencies)

The 14 'Prioritised opportunities' have been worked up into more detailed feasibility documents to understand the cost and resource requirements of implementing vs value add

The support model for Success Factors will continue to be reviewed to look for opportunities to speed up delivery of enhancements at a reduced cost

The HRSC Director will have a focus on creating an optimal delivery structure with clear roles and responsibilities and increased capability to deal with system improvements – building on the formal accredited system training currently available

Development of HR dashboards underway – improving MI quality and reporting capabilities

POL00401629

Summary of Activity Findings (Focus Areas – Determined by 'Value Add')

The 22 opportunities identified by Deloitte as 'Priority' based on value add have been 'combined' and worked up into 14 'prioritised opportunities that will form focus areas for POL as the HRSC is developed (It should be noted these were not necessarily quick win or low cost to implement and some rely on further development of the HR TOM - therefore implementation is staggered)

	Prioritised opportunity	POL Activity	Approx delivery date	Owner
1	Optimise System Role Based Permissions in SuccessFactors	Role Based Permissions are being reviewed alongside the process improvement work (new processes will be defined that will identify the optimum RBP set up)	Inflight and ongoing	Responsibility for delivery of the process improvement workstream and delivery of the SF system improvements will sit with the new HRSC Director (Starts Sept 20)
2	Improve People Data Configuration in SF	This is a mix of small changes and more complex development. Ongoing programme to update and make small changes through Accenture Support – requirements sit alongside incoming ad hoc 'fixes' and urgent requests	In flight and ongoing	
3	Improve Advice Centre Tiered Structure	Recommendation for tiered Advice Centre Structure an output of the Process Improvement work – maximising use of technical solution to reduce incoming requests	In flight & part of HR TOM	
4	Development of System Knowledge Capabilities	Formal development for the SF internal support team now available through the SAP / Success Factors Learning Zone. Training to form part of Process Improvement stream Team capability to be reviewed in POM T2 activity	In flight & part of HR TOM	
5	Review SF development / support contract	Accenture contract To be discussed with procurement to understand if more value can be obtained from existing contract	Q4	
6	Build out the HR/IT Systems Governance and Innovation Forum	Post HRSC TOM / T2- Current forum responsibilities to be reviewed to support governance for change requests, system updates and release management, moving key decision making and activity prioritisation in-house (needs to be in conjunction with point 5).	Q3	
7	Automated System Alerts for Absences & Stage Warning	Complex triggers at POL make automated alerts impossible. However, a new solution has been agreed with Employee Relations, empowering managers to manage the process and making use of system 'pop up' messages and reminders to support (Trial planned from 01/10)	In flight and ongoing	

Work started | On track | On Hold (due cost or priority)

Key control mechanism for monitoring performance, future development & BAU updates

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

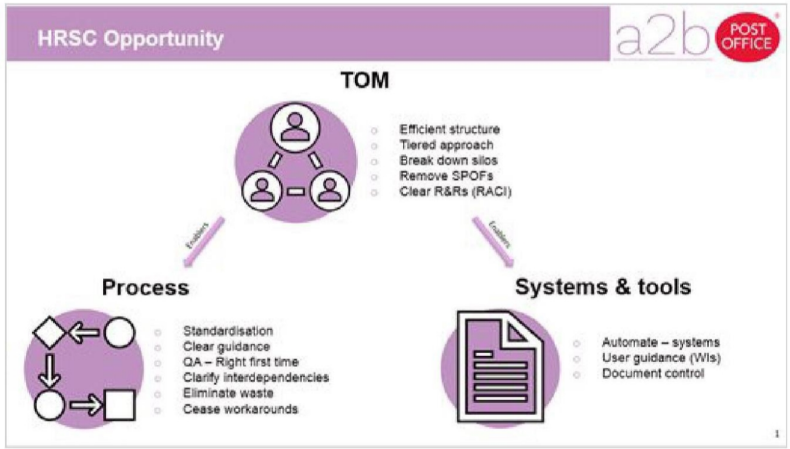
Summary of Activity Findings (NEW)

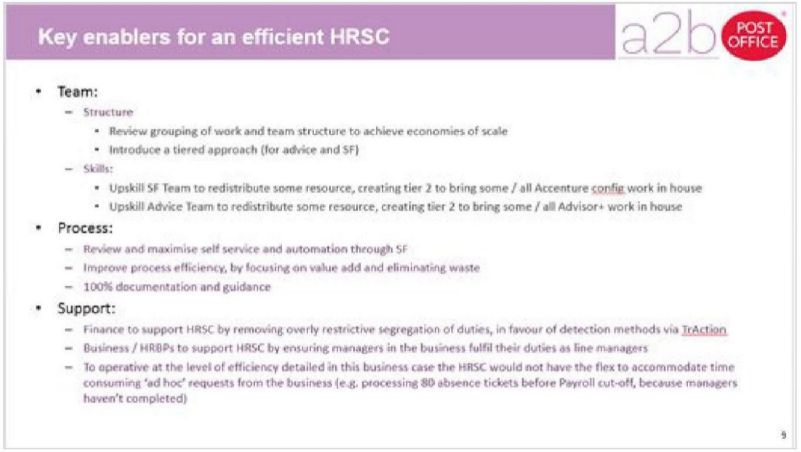
	Prioritised opportunity	POL Activity	Approx delivery date	Owner
8	Redesign Employee Relations operating model	On hold subject to completion of HR TOM – Needs full scoping - likely to require additional funding as will require significant configuration to enable SF to capture Employee Relations data and enable self serve (costs will be offset slightly by ending the partnership with AdvisorPlus. To maximise value use of chatbots and other automated tools could be explored.	On Hold – review in Q1 '21	Responsibility for delivery of the process improvement workstream and delivery of the SF system improvements will sit with the new HRSC Director (Starts Sept 20)
9	Perform End to End Onboarding Review and introduce automation to contract production and vetting processes	Work to simplify structures and get greater alignment across POL around contracts has started. This will be the key enabler for automated contract generation and vetting processes. This opportunity will require investment and will continue to be reviewed after the enablement work has progressed further, potentially in Q1 '21-'22	In flight and ongoing	
10	Digitisation of Consultation Packs & Leaver Letters	Aiming to have packs digitised for end of Q3. Solution worked through for payslips, p45s and accompanying letters	Q3	
11	Introduction of a full suite of HRSC and wider People Team SLAs	This will form a key objective for the new HRSC Director and will also form part of the HR TOM	Q4	
12	GDPR qualification. Processes and data flow are impaired by an overzealous interpretation of GDPR	GDPR compliant, but practical changes to RBP (Point 1) will form part of the process improvement work. Currently a single process can have multiple handoffs within a single team, with each person having a different access permission. Risk would be lowered by having a smaller number of multiskilled system admins managing multiple processes and data requests – Fewer people = more secure / more efficient	Q4	
13	HR Team mapping to processes with clear RACI	This will form part of the HR TOM work on the back of the wider POM activity. Likely to fall in Q4	Q4	
14	Optimise the Payroll & Pensions processing cycle	P1 and P2 payroll processes identified and work on some P1 activity has commenced. Forms part of the process improvement work which is also filtering into Project Assurance	In flight and ongoing	

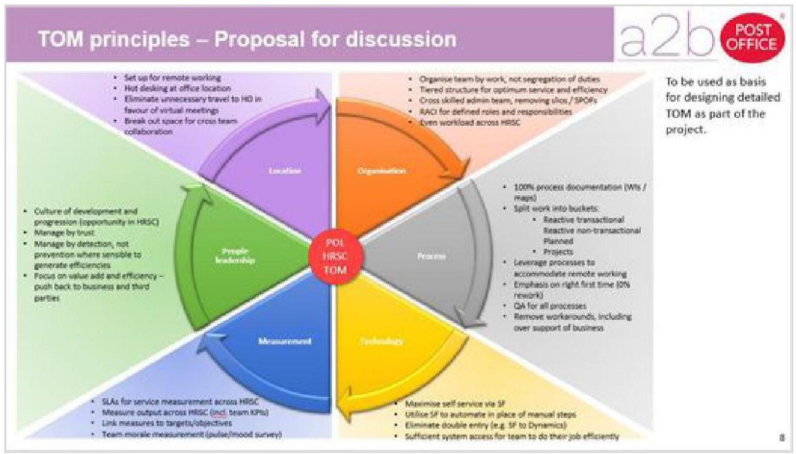
Work started	On track	On Hold (due cost or priority)

POL00401629

Process Improvement Workstream







The Process Improvement Workstream includes:

- Ground up, detailed process review and development
- Development of HRSC TOM
- Development of the Deloitte 'quick wins'
- Role based Permission (RBP) Review
- Capability build and system training
- LEAN process roll out
- introduction of governance to monitor future process development

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Summary of Activity Findings (Quick Wins)

✓ = Completed WIP = In progress ⧗ = Awaiting planned kick-off

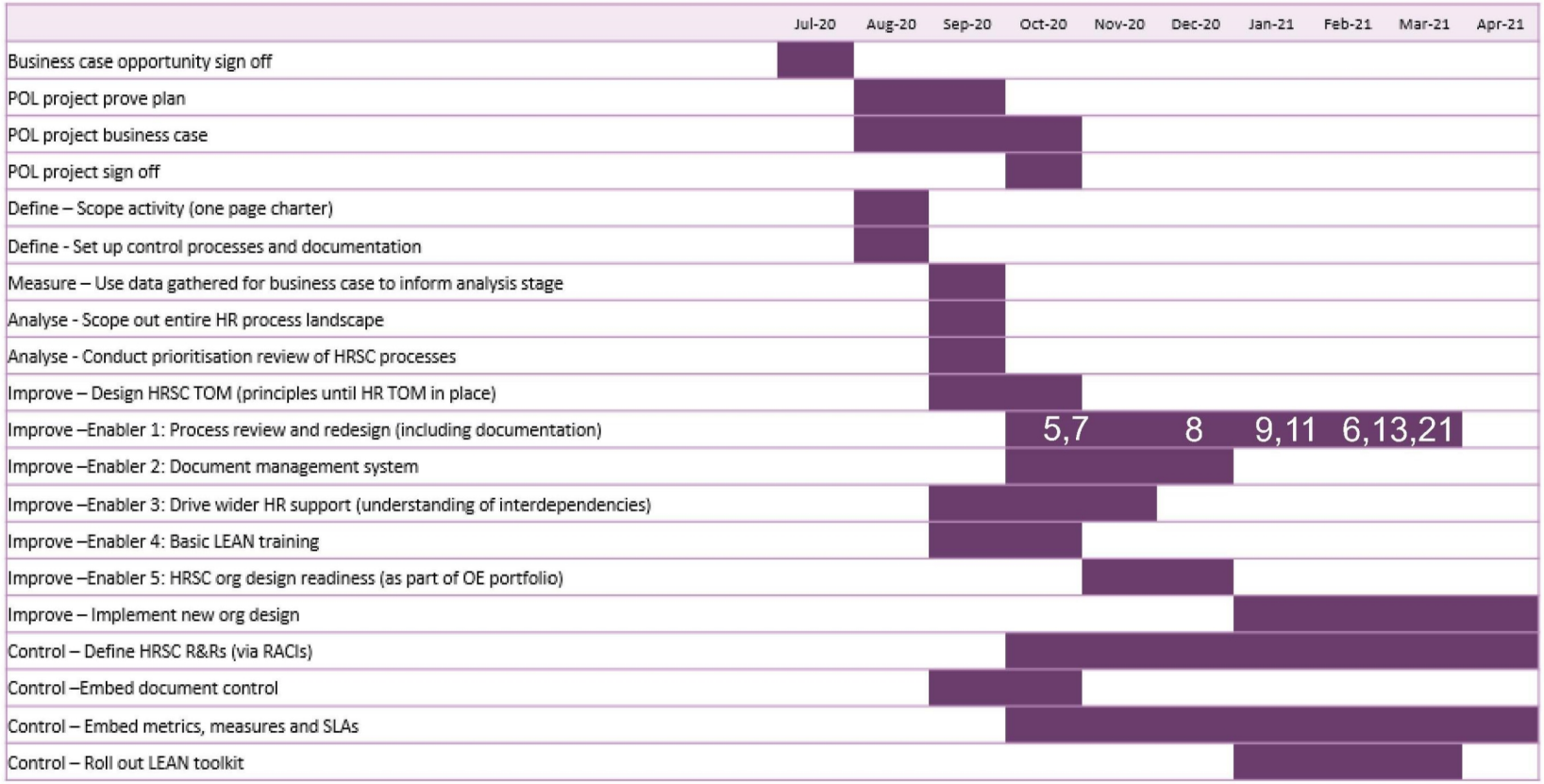
Of the 51 opportunities identified by Deloitte, 21 were 'quick wins' which could be delivered relatively easily with minimal cost. Each of these 'quick wins' has been factored in to the Process Improvement workstream and have been worked into the timeline – Some actions – like, improving data configuration, RBP and notification changes will be adopted alongside the review and development of each process and therefore will be actioned over the lifespan of the wider project. 'Go live' of each element may also be dependent on the Accenture roadmap, resource availability and other changes that may occur as a part of the wider TOM development

	Quick Wins		Quick Wins
1	Enable employee probation alerts ✓	12	Alignment of SF release to business needs ⧗
2	Improve people data configuration WIP	13	Review of SF notifications WIP
3	Install a pool laptop for supply chain staff ⧗	14	Optimise org restructure process ⧗
4	Prevent / stop calls to the advice centre ✓	15	Automation of Settlement Agreement Packs ⧗
5	Connect job-level to base compensation ⧗	16	Review HRSC and POL roles and responsibilities WIP
6	Automation of pay progression processes ⧗	17	Automate system alerts for absences WIP
7	Automation of leavers termination date ⧗	18	Automate payroll validation and testing of exceptions ⧗
8	Optimise system Role Based Permissions (RBP) WIP	19	Enable a notes page for the payroll team ⧗
9	Build out HR / IT governance and innovation forum ⧗	20	Review management approval process for personal requests ⧗
10	Review Accenture roadmap and support contract ⧗	21	Enhance business rewards processes WIP
11	Development of system knowledge capabilities ⧗		

POL00401629

Proposed Timeline for Process Improvement Workstream

Timeline includes anticipated delivery for some of the key quickwins. Some of the quickwins - like notification updates, will be applied alongside each individual process review and will last throughout the lifespan of the workstream (Numbers correspond with quick wins from last page)



Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Considerations and Risks Regarding the Future of Success Factors

- Post Office has invested significant money, time and effort to date in Success Factors – and the system *is* delivering benefits. Any suggested alternative HRIS would require significant investment without there being any guarantee that the service delivery or efficiency would be improved
- Bringing in any alternative system before addressing the issues that created the problems within Success Factors will set us up to fail and sink more funding. The complexity of the existing set up (data and processes) makes moving to another system or outsource provider extremely risky at a time when the business is focussed on other priorities
- There may be other opportunities to reduce running costs. Existing contracts should be challenged around licences and the support model – we may be able to leverage more value from the existing set up with less effort and need to reduce the reliance on a 3rd party for small enhancements
- If we want to maximise returns from the system, further funding may be required in the short term to speed up delivery of changes that will ensure regulatory or legal compliance or enhancements and changes that could deliver greater value / ROI in the longer term. Ongoing development is included in the current overall tech enablement budget for OE covering small developments. Any significant additional development will be costed and assessed against value add – before work commences (which may change the delivery plan)
- Whilst SF is primarily an HR system, other functions, such as IT and Finance will need to be actively involved in the decisions around it's development and future role.
- The TOM for the HRSC should be outlined before any long term decisions are made on the future of SF. The SF development plan will need to run alongside the development of the HRSC TOM
- In April '20 the current SF contract was extended by 2 years to April 22. Time did not allow for a full procurement review and activity around Covid 19 took priority in both HR and IT
- The procurement process for sourcing any alternative is likely to take 12 months – which would result in the existing issues being 'lived with'. It would delay the full implementation of the HR TOM until the new system was developed to support – otherwise we risk a new structure and ways of working being hampered by existing technology we are not able to invest in

POL00401629

Recommendation

The ARC are requested to agree to the following recommendation relating to the future of SF @ POL:

Short / Medium Term (1-2 years)

At the current time it is recommended that in the short/medium term, Success Factors remains the central HR tool around which process improvements and the future HR TOM is built. It is delivering core HR services and, work underway now to simplify HR operations will provide a solid base on which to enhance and obtain more value from the system – although this may require some additional funding in the short term – which could determine / alter the delivery timeline. The introduction of a dedicated HRIT Governance & Innovation Forum alongside the existing HRSC governance processes will add increased rigour and control to the development and BAU operations of the system.

Long Term

It is recommended that we carry out regular 'Heath Checks' on Success Factors and that it is reviewed again in one year – allowing the current organisation change and efficiency projects (POM) to begin to take effect. At this point, we will have started to implement a simplified organisation with a reduced headcount and increased alignment across HR T&Cs and ways of working. The HRSC will be operating more efficiently and will have a clear view on whether the technology is meeting requirements or not.

This 'Health Check' will be an early indicator to show if Success Factors can continue to meet the needs of the business in the longer term. If a decision is taken to look at alternatives, we can do so, knowing that many of the complexities that have resulted in the issues experienced in the initial implementation will have been resolved – making further development of SF OR implementation of an alternative HRIS much more likely to succeed.

POL00401629

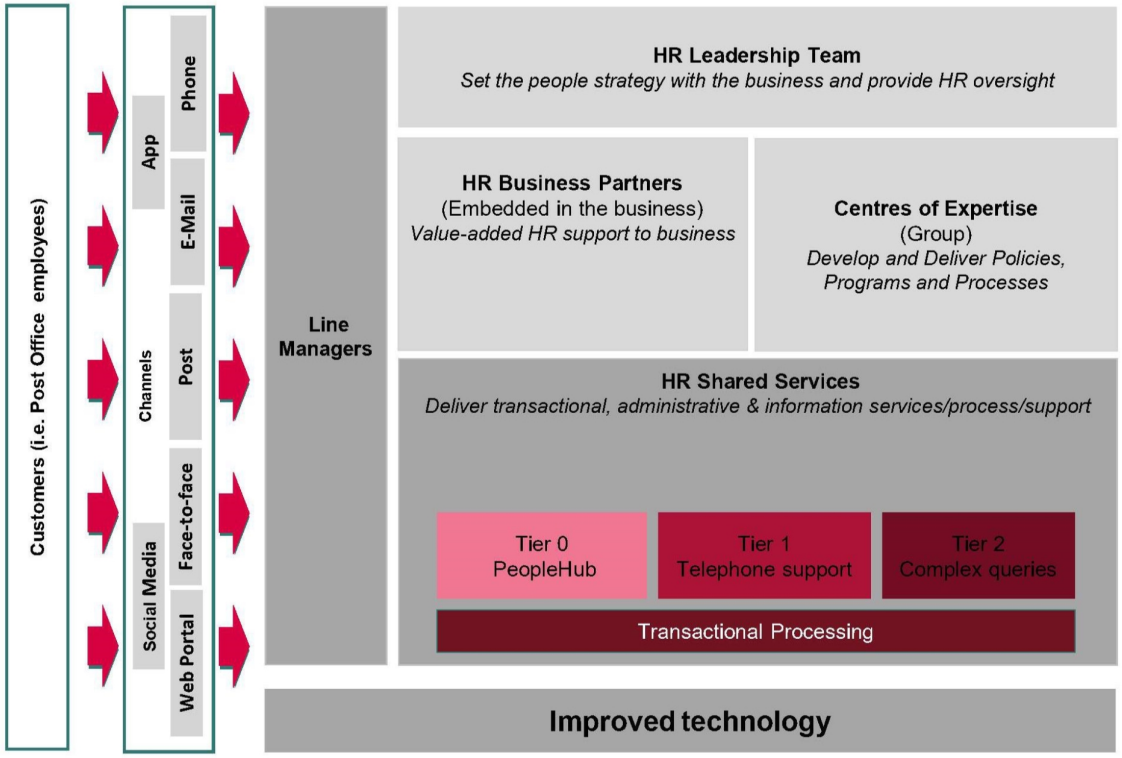


Appendix

POL00401629

HR TOM 2020 – UNDER DEVELOPMENT

In 2020 the HR TOM will continue to be developed and implemented on the back of the wider POM programme. It will continue to be based largely on the model below which is widely-accepted best practice, and is in use by similar sized organisations. Our task is to build on the foundations already in place to improve service delivery and efficiency in tandem.



Customers will access HR support tailored to their needs – through efficient self-service and up-skilled line managers, to more specialist help as required. Improved digital channels as well as telephone and face-to-face support will be provided.

Our tiers of support will be:

The **HR Leadership Team** sets the people strategy which aligns to the PSG ambitions

HR Business Partners provide value-added support to their business area

HR Centres of Expertise provide expert advice on their specialist area and develop and deliver specific policies, processes and support and addressing any queries that cannot be resolved in Tier 2

HR Shared Services operates three levels of service:

Tier 0 – Online self service via the PeopleHub

Tiers 1 & 2 (HRSC & Outsourced Services) provide administrative and transactional support to all employees, from first-point-of contact to more complex queries, and processing e.g. Payroll, Recruitment

Line Managers provide initial support to colleagues, supported by manager self-service, **and** HR

Improved technology underpins the whole model.

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Current Change Control Process for HR Systems (Overview)

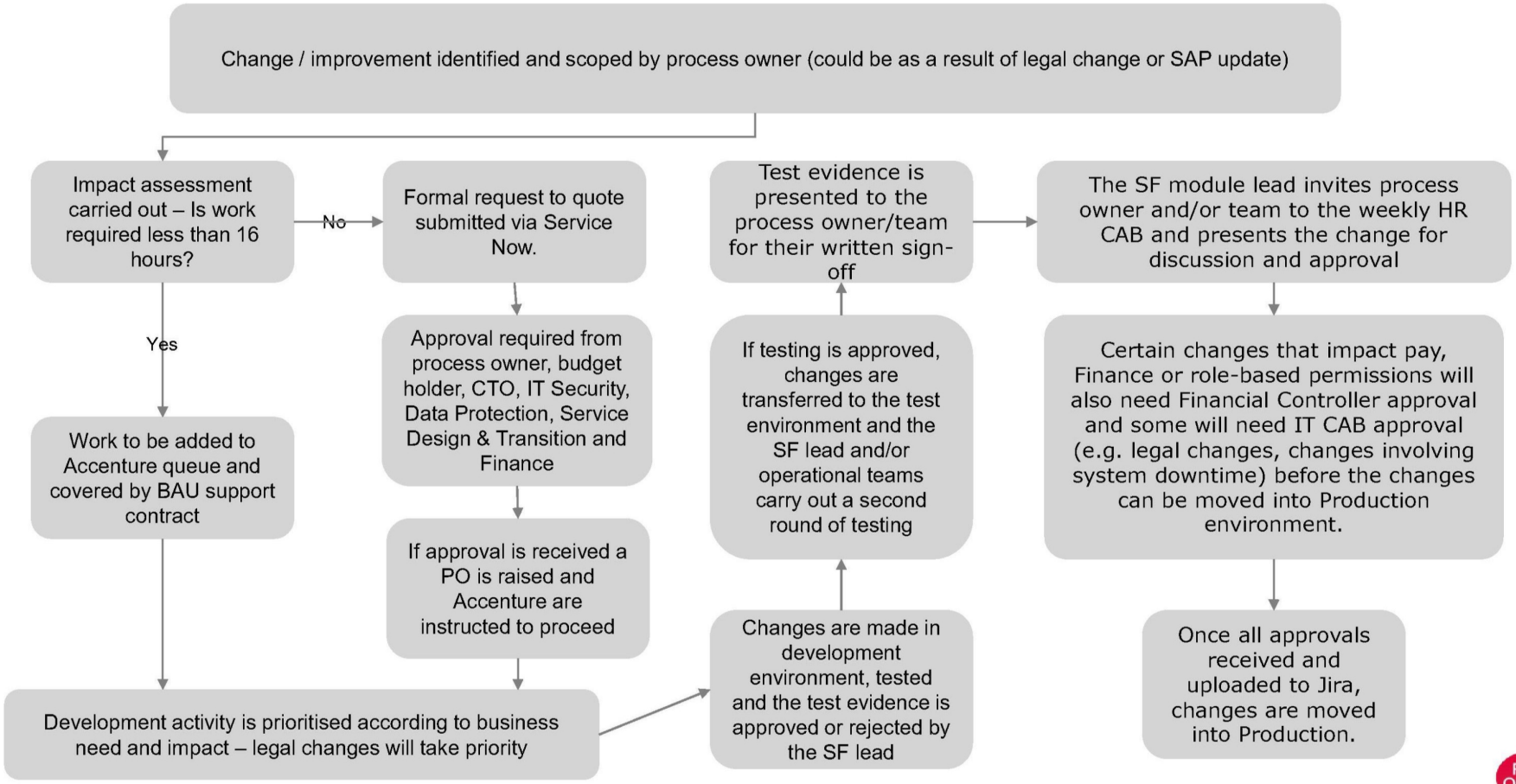
- CR raised and approved including scope and justification
- CR approved & signed off by sponsor
- Data Protection approval received (if required)
- Ticket raised through Jira *(A Jira ticket is the logging tool between POL & Accenture)*
- Discussed at HRCAB (Human Resource Change Approval Board) for Impact assessment (IA)
- Head of HRSC, Change & Integration & HR Systems & MI Mgr approve/reject following IA (IA explains the approx. cost of the work and solution)
- Approval given - lower environments configured and fully tested and documented
- Weekly HR CAB meetings held – (Made up of :-Change & Integration Mgr, HR Systems & MI Mgr, SF BAU team & Accenture) and approved to move in *Prd (minor changes) *Prd is our Live EC system
- Weekly iT CAB meeting approve major changes



Change Request form HR Systems

POL00401629

Current Change Control Process for HR Systems (Detail)



POL00401629

Key Lessons Learned From Initial SF Implementation

In March 2018, the Change Assurance Report carried out a 'Lessons Learnt Review' which fed into the FY17-18 Annual Audit Plan (approved by ARC). The aim was to understand the issues that occurred and the reasons for the delays and overspend. The key themes of the issues highlighted were:

Design – There was a lack of overarching governance in relation to the solution design – There was no Design Authority in place and no formal review of the high level design and detailed requirements. Certain functionality requirements were missed as an impact analysis was not carried out.

Testing – Poor test approach identified and a lack of compliance with the test strategy. Test scripts were not detailed enough

Data – The process for loading data into SF continually changed – migration was hindered by poor data quality

Specific areas of concern identified - regarding the management of the project included:

Project Planning

1) Lack of in-depth planning prior to project initiation
2) Absence of a resource management strategy

Project Performance

3) Ineffective test governance

Project Governance

4) Non compliance with project governance requirements
5) Lack of alignment between contractual documentation and project deliverables

Raid Management

6) Inconsistent RAID management and lack of third party risk strategy

It has since been noted that some of the SF1 Gating Go/No Go documentation has gone missing. This appears to have happened during a transfer of the documentation.

2020 Response:

Since the original implementation, there have been changes in leadership and delivery teams within both HR and SPO. New processes have been implemented to prevent a repeat of the issues raised and ensure strong governance across all aspects of programme management. **An update to the ARC, detailing the processes and controls which have been implemented across Change is planned for November '20.**

POL00401629

Deloitte Review - Opportunities Long List – People (1/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
1	Advice Centre, Recruitment and Administration	P0002	Enable Employee Probation Alerting	This opportunity is directly related to Technology / Automation. What: Ability to provide alerting around probation end, with automated email sent to line management to ensure a compliant process. Auto-Escalation to HRBP after a set amount of time. Why: Lots of time spend within HRSCs on monitoring End of Probation and contract extensions. How: System to Proactively inform Line managers on their responsibility to follow up on contract updates
2	Advice Centre, Recruitment and Administration	P0004	Improve People Data Configuration	This opportunity is directly related to Process, People and Technology / Automation. What: Improve the existing People Data Configuration in SuccessFactors Employee Central (Core HR) Why: Due to incorrect configuration and/or outdated foundation tables the system is automatically prompting incorrect data based on Data Changes that need to be corrected by HR Admin after completing the request. How: Currently a number of SF design improvements for example:- Upload of current rate tables - FTA contract (10 hour) leading to automatic input of incorrect inner / outer London waiting allowance - System alert for incorrect data input - automatic pro-rate salary - Salary set up e.g. £20,000 set up at £19,997.
3	Advice Centre, Recruitment and Administration	P0006	Rebrand and Launch PeopleHub	This opportunity is directly related to Technology / Automation and Data. What: Develop current internal HR tool / knowledge base to capture incidents picked up by the Advice Centre through the call centre. For example, referring members to policies applicable to their contract, payroll queries, password resets etc. through improving the navigation on the PeopleHub site, or improving the search functionality by adding tags to articles Why: Improved Service Delivery to end-users and reduced workload on Service Centre. How: Leveraging the possibilities and awareness of PeopleHub capabilities.
4	Advice Centre, Recruitment and Administration	P0008	Improve Advice Centre Tiered Structure	This opportunity is directly related to People, Process and Technology / Automation. What: Creation of a tiered structure (Level 1/2) for the Advice Centre through the use of Robotics which faces off into the wider Post Office business. Why: Current processes to answer to inbound HR queries are repetitive and inefficient and can be structured more efficiently How: Leveraging Chabot's / ServiceNow / PeopleHub as a level 1, with expertise (human) support from Level 2 onwards
5	Advice Centre, Recruitment and Administration	P0035	Implementation of New ER Operating Model	This opportunity links to People. What: Currently, managers use AdvisorPlus for employee relations advice and guidance. Why: This service will not no longer be available once the contract runs out, and therefore managers need to be coached / trained on future employee relation advice that they may need to provide and be aware of. In addition, HRBPs up-skilled to provide advice on employee relations enquiries. How: Upskilling line managers to be able to handle certain employee relation activity. A new Operating Model aligned towards self-service to be implemented.
6	Advice Centre, Recruitment and Administration	P0036	Connect Job Level to Base Compensation (Non - Management)	This opportunity links to Data and Technology / Automation. What: When assignment of job level in recruitment / administrative changes, there is a lack of, or incorrect connection between job level and base salary. This directly effects all non-management staff. Why: There is a manual pro-rata for salary and holiday. How: Amend SuccessFactors to allow for change to the base salary each year, which can then be automatically updated for new and existing employees.

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Opportunities Long List – People (2/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
7	Advice Centre, Recruitment and Administration	P0044	Automation of Pay Progression Process	This opportunity is directly related to Process & Technology / Automation. What: Currently, salary progressions are done manually, with no automatic configuration. Why: The team on the ground is currently running an excel analysis, checking who require a salary progression, sending an email to the manager to confirm and make the adjustment. Upon completion, a letter of agreement is shared with the individual which is completed manually. How: Automation of pay progression based on automated alert raised to the team for individual close to their probation / scheduled date, to process pay progression case.
8	Advice Centre, Recruitment and Administration	P0045	Automate New Hires Contract Generation	This opportunity is linked directly to Technology / Automation and People. What: Currently, contractual agreements for new hires are created manually. Why: Data is transposed from SuccessFactors and other systems, causing a number of repeated steps in the process. How: Automating a number of the reports, will reduce a lot of the manual effort, as fields pulled from SuccessFactors is the same, but differs per individual.
9	Advice Centre, Recruitment and Administration	P0050	Install a Pool Laptop for Supply Chain Staff	This opportunity links directly to People. What: Post Office staff (deport staff) face difficulties accessing technology platforms where a number of issues / enquires could be answered. How: Where availability to laptops might be limited, installation of a pool laptop at each of the locations so employees are able to log into SuccessFactors would alleviate a number of incidents that are picked up by the HRSC. For instance, incorrect overtime hours, sick pay, absences etc.
10	Advice Centre, Recruitment and Administration	P0051	Prevent / Stop Calls to the Advice Centre	The opportunity links to People & Process. What: Currently, a percentage of staff are spending their time reviewing phone call enquires, with sufficiently large volumes monthly. Why: Typically, the business refer staff to policies that are available to read on the PeopleHub. A sufficient amount of time is spent explaining content, where it can be accessed through digital tools. How: By stopping calls, this will introduce a self-service mind-set across the business.
11	Advice Centre, Recruitment and Administration	P0052	Perform Process Review and Lean Simplification of Requests	This opportunity links to Process. What: Currently, the HRSC are receiving a number of different requests concerning the individual, spanning from learning to purchase orders. Why: The advisers within the HRSC are seen as the call-centre for the rest of the business. How: A review of the request types from the business to the HRSC to confirm time taken to provide input and response to each request type.
12	Advice Centre, Recruitment and Administration	P0053	Enable Workflow Tool to Manage Requests for Advice Centre	This opportunity links to Process and Technology / Automation. What: Currently, the team are receiving multiple requests via email and call for learning and development, room bookings, course enquires, which are all handled over phone, and passed through to respective HRSC departments. Why: Efficiencies are lost in drafting emails, sharing information with relevant departments occur due to lack of digital tool to support queries. How: Introduction of ServiceNow would accommodate for a workflow where queries can be handled succinctly.

POL00401629

Opportunities Long List – People (3/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
13	Advice Centre, Recruitment and Administration	P0056	Perform a review of the end to end Onboarding and Recruitment Process	This opportunity links to People and Process. What: Review the E2E Recruitment & Onboarding Process on manual process steps and (duplicate) data entry Why: Currently, there is a number of paper and digital transactions taking place and it is unclear what the hand-off points are between HRSC and Post Office stakeholders. How: An analysis of the existing end to end on-boarding and recruitment process will drive efficiencies not realised currently. Also take into account the latest release from Onboarding 2.0 and the additional benefits for automation / data processing
14	Advice Centre, Recruitment and Administration	P0058	On-boarding engagement for new recruits to be improved	This opportunity links to Process. What: Exploring the user-journey for new employees to be on-boarded by Post Office is currently not the optimum as described through voice of the customer interviews held. Why: Currently a new recruit when joining the Post Office can quickly become disengaged due to lack of 'just in time' training, supporting videos and flowcharts that would help if present, them navigate efficiently through their first few days/weeks. There is a lack of understanding when it comes to using SuccessFactors and inductions can be inconsistent. How: A project has been kicked off to address the issues and some of the opportunities that have been captured during this review will support the On-Boarding goal.
15	Change and Integration	P0010	Introduction of Exit Management Portal	This opportunity is directly related to Process and Technology / Automation. What: Improvement of the Exit Management Process and the Introduction of a Exit management Portal. Why: This enables a alumni population/network (not using personal email addresses) and leaver's checklist. Additional opportunity for annual leave checks, IT kit for generating communications, and calculating holidays into Success Factor. How: Automated packs to send payslips / P45; identify business rules for auto-calculation of leave days in SuccessFactors
16	Change and Integration	P0011	Automation of Settlement Agreement Packs	This opportunity is directly related to Process and Technology / Automation. What: Automation of Settlement Agreement Packs Why: A lot of time is currently spent on processing the information for the pack as information is pulled from SuccessFactors and then manual calculations are performed. In addition, there is an opportunity to automate signatory acceptance. This is currently paper based and it takes full days to put together the settlement agreement packs. How: Achieve automation including the mail merge of document packs and electronically sending documents (statutory agreements) to individuals and to legal counsel.
17	Change and Integration	P0037	Apply Automation to Employee Reference Request Process	This opportunity links to Technology / Automation. What: Currently, Post Office must capture an employee's agreement to have a reference check. Why: When an employee leaves the business, their new employer will reach out to Post Office to request for a reference from the business, This can not be processed without the consent of the employee. How: To reduce the manual effort to have a reference checks authorised by the individual concerned once they have left. This can be leveraged by a simple tick box in SuccessFactors when on-boarding an employee.

POL00401629

Opportunities Long List – People (4/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
18	Change and Integration	P0046	Digitisation of Consultation Packs & Leaver Letters	This opportunity links to People, Process and Technology / Automation. What: Consultation packs, which are set templates, are printed out each time Post Office members are made redundant. Why: Consultant packs are printed, sent to the Operations Advisor, sent via Royal Mail special delivery for signatory acceptance, which is then sent back to the Change team. Paperwork is also stored externally in Oasis, a cost that the business is incurring. Once consultant packs have been received, a Settlement Agreement is then sent to the employee. How: Digitisation of initial consultation pack to reduce costs incurred of sharing standard draft document with the operations advisor.
19	Change and Integration	P0049	Automation of Leavers Termination Date	This Opportunity links to Technology / Automation. What: Currently, there are number of multiple screens in SuccessFactors that need to be updated with the termination date - this has to be manually updated. Why: For instance, if the leaver had a company card, the team would require an input of the end date in SuccessFactors. How: The termination date does not pull throughout the entire system.
20	HR Systems & MI	P0001	Optimise System Role Based Permissions	This opportunity is directly related to Process and Technology / Automation. What: Optimise the role based permissions in SuccessFactors for all roles within the HRSC. Why: Lots of processes (e.g.. Pay Related) require involvement from different HRSC Team members with different permissions. This is reducing the turn around time per process. How: Focus on trust-based elements by giving administrators access to the full dataset of Job/Comp Information covering their workflows in 1 step.
21	HR Systems & MI	P0003	Consolidate Third Party People Data	This opportunity is directly related to Data and Technology / Automation. What: Enable SuccessFactors add-on to consolidate 3rd party people data across the Post Office and have one source of truth. Why: Currently data from Contractors / contingent workforce is held on separate systems. Contractors are managed by Sopra Steria and data managed by AdvisorPlus for Payzone and HR Online for Post Office Insurance. How: Enabling the Contingent Worker functionality in SuccessFactors EC module would allow Post Office to maintain a 'light' profile of these external workers next to the 'full' profiles of regular employees
22	HR Systems & MI	P0012	Optimise Organisational Restructure Process	This opportunity is directly related to Process and Technology / Automation. What: Optimise the Organisational Restructure Process by enabling mass changes to Organisation & People Data Why: The recent reorganisation requires mass data changes to be made in the system to individuals' divisions and departments. This is a manual task, requiring each individual's profile to be updated one by one. The foundation data to be updated with help of Accenture due to wide-reaching impacts and necessary changes to resolve issues, e.g. for RBPs and workflows. How: Opportunity to identify the functionality of mass data changes for Foundation and People Data within SuccessFactors

POL00401629

Opportunities Long List – People (5/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
23	HR Systems & MI	P0014	Development of System Knowledge Capabilities	This opportunity is directly related to People. What: Improve SuccessFactors and Reporting knowledge capabilities within the HR Systems and MI Team. Why: Building a knowledge network within the Post Office will reduce the dependency on Vendor capability and will create efficiencies and self-driving teams in terms of System defect management, change request optimisation and Report Creation How: Greater access to be granted in the Development system in order to execute more tasks independently of the AMS vendor. Leverage the SAP knowledge Portals; Identify need for SuccessFactors Certification training.
24	HR Systems & MI	P0015	Enable Proxy (act on behalf off) Access for SuccessFactors users	This opportunity is directly related to People and Process. What: A governed process / approach for Proxy Access (acting on behalf of) needs to be defined as this is currently not well defined within Post Office. Why: Enabling Proxy rights to specific roles within Post Office (HRSC or the Business) will drive process efficiencies; as roles can act 'on behalf of' in order to complete data changes / workflow tasks How: Identify who currently have Proxy Rights, which roles should preferably have proxy rights and update the Role Based Permissions accordingly
25	HR Systems & MI	P0016	Revisit Global Data Definition	This opportunity is directly related to Data. What: There should be a People Data Definition Owner that owns the SuccessFactors data model and is able to provide unique descriptions on field level details Why: When consolidating data pulled from different data sources it is important to apply a Global Data Definition to ensure data can be compared and analysed in the same way How: Define Data Definition Owner and identify known differences between current HR Data Sources and seek for harmonisation
26	HR Systems & MI	P0018	Review Business Reports to Reduce Reporting Requests	This opportunity is directly related to Process, Technology / Automation and Data. What: Consolidate number of business reports to meet stakeholder needs and demands Why: Currently lots of reports are created and shared towards the HR Business Partners and Directors community that are not always required / do not include the right amount of information in order to drive business decisions How: Overview of total list of reports shared towards the community; define redundant reports and define new reports (consolidate information from different areas within SuccessFactors)
27	HR Systems & MI	P0019	Setup System Support Users for SuccessFactors	This opportunity is directly related to People. What: Enable SuccessFactors-users to create and own Support tickets and increase role based permission rights within the system to leverage the current service contract with Accenture. Why: Currently the team is depending on Accenture for handling HR change request, new initiatives and defects where they also would be able to research and handle business requests themselves directly with SAP How: Education on SAP-User creation; how to log tickets in the right manner at SAP and where to access Product Documentation

POL00401629

Opportunities Long List – People (6/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
28	HR Systems & MI	P0020	Review Accenture Roadmap & AMS Contract	This opportunity is directly related to People & Process. What: The Governance Model on HR IT (SuccessFactors) support must be revised. Contractual decisions on RACI between Post Office People, IT and Accenture to be clarified. Why: Current support contract with Accenture disallows the Post Office team to be self-driving and is causing significant delays in resolving defects and processing change requests not fulfilling the current HR Business requirements which negatively impacts the user experience throughout the HR Community How: Review current Governance Model and identify opportunities for improvement towards current contract and setup of SuccessFactors
29	HR Systems & MI	P0021	Introduce CAB Forum for People Systems	This opportunity is directly related to People & Process. What: Review the Change Approval Board (CAB) Governance and outline the process for required system changes. Streamline the forums and review required attendees. Why: Particular need for greater and earlier involvement from key business stakeholders feeding in the requirements for change within SuccessFactors. How: Which stakeholders are currently involved in the Change Request process; which stakeholders should be included in the To-Be State (Clear representation from Business HR) and how often are SuccessFactors Release Updates shared throughout this community
30	HR Systems & MI	P0032	Review of SuccessFactors System Notifications	This opportunity links directly to Data and Technology / Automation. What: A number of system notifications could be leveraged to support line management with a number of their responsibilities, send notifications where action is needed. Why: HRSC are having to complete a number of re-work activities on a number of cases where line management have not completed the task. How: Audit / review all SuccessFactors notifications sent out from the system to identify where: A) link to pages on PeopleHub. B)Improve quality, clarity and timing of the message – which includes any escalated notifications to i.e. second line manager or HRBP. An example of a good automated notification which would help (particularly Luke in HRSC) would be a weekly automated email which is sent to a line manager when a direct report has a live sick absence on the system reminding them (just in case they haven't closed the absence on SF) and highlighting things like PeopleHub / OH assist for referrals and the Sick Absence Policy.
31	HR Systems & MI	P0033	Redesign of SuccessFactors Performance Module	The opportunity links directly to People, Data and Technology / Automation. What: Review the performance module on SuccessFactors. Why: Business users are generating a lot of noise from stakeholders that the form is clunky and the stages don't flow in the right order. How: Perform a review of the module and map to business requirements to identify gaps.

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Opportunities Long List – People (7/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
32	HR Systems & MI	P0040	Alignment of SuccessFactors Release to Business Needs	This opportunity links to Technology / Automation and Process. What: Currently, SuccessFactors release notes are not translated from technical language into business language, therefore, opportunities to improve user experience within system design is missed. Why: Current vendor outlines the Release Updates solely on technical impact without translating this to the business impact. Within PO HR System Team there should be capabilities to add this perspective and share into a wider business group (possibly to be formed) How: Review SuccessFactors (bi - annually) release cycle and align towards business needs and requirements, to address where these can be met. This could be explored in CAB forums led by the SuccessFactors HRSC team.
33	HR Systems & MI	P0041	Configuration of PowerBI to Natively Integrate with SuccessFactors	This opportunity links directly to Data and Technology / Automation. What: Currently SuccessFactors does not natively integrate into PowerBI (fully licensed). Why: Within PO there is the need for report creation through consolidating different HR data sources (Core HR, Payroll, Finance) currently involving lots of manual work around in doing so How: Explore back-end configuration of SuccessFactors, understand requirements of business reports, and pull data from system
34	HR Systems & MI	P0042	Introduce Analytics & UX Reporting across the Business	This opportunity is directly related to Technology / Automation and Data. What: Business staff are waiting too long (c.3-5 days) for data to be sent to them based off their request. Why: Enable business staff across Post Office business to access live dynamic dashboards. How: Enable the use of dashboards for business users, which will allow for key business metrics to be tracked for Post Office business teams.
35	HR Systems & MI	P0043	Improve Current System Stability and Quality	This opportunity directly links to Technology / Automation and Data. What: When running reports, the system frequently falls over and increases time taken to capture information and drops data. Why: This means reports are not complete and can not be used as required by the business. How: Address system capability needs to see where system servers can support and investigate the dynamics of Permission Groups that can impact the number of results on a report.
36	HRSC	P0039	Retrain Line Management on SuccessFactors and PeopleHub	This opportunity links directly to People and Technology / Automation. What: Due to the incorrect use of the technology enabled tools in Post Office, there is a number of incidents with absences, over payments, overtime, leave, sickness. Why: This is due to the lack of upskilling with line management staff on a number of the Post Office digital tools. How: This can be enhanced by on the job training. Training could be delivered via webinars, e-learning, one to ones, on-boarding sessions and super users (business led).

POL00401629

Opportunities Long List – People (8/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
37	HRSC	P0047	Introduce Service Level Agreements for the HRSC	This Opportunity links to Process. What: Post Office business stakeholders unclear on activities happening with HRSC and elapsed delays when requests are sent to the team. Why: Unable to measure the performance of the HRSC function. How: Establish Service Level Agreements between HRSC and its customers both within the People function and across the wider business to introduce measurable performance metrics of the HRSC function.
38	HRSC	P0048	Review POL GDPR policy and risk tolerance	This Opportunity links to People. What: Where personal data requires accessing, HRSC staff have to reach out to the Information Security team to request for approval. Why: A number of GDPR led policies in place which limit the teams ability to work efficiently and quickly to address a number of business - related enquiries. How: Review the GDPR policy across the Post Office, to develop appease the risk appetite of the team currently supporting the business in HRSC.
39	HRSC	P0055	Increase Efficiencies between HRSC and POL	This opportunity links to People. What: Post Office business stakeholders have shared their view on time it takes for HRSC to complete a number of key HRSC processes. Why: Could be related to Technology, Process or Knowledge Capabilities How: To alleviate some of the lag - time experienced, a review of current ways of working and relationships between the HRSC and business staff to be conducted. Efficiency gains can be achieved through enhanced relationships and improved ways of working between counterparts.
40	HRSC	P0057	Review HRSC and POL Roles and Responsibilities	This opportunity links to People and Process. What: Perform a review of HRSC and Post Office business stakeholders key roles and responsibilities where there are inter-dependencies. Why: This is to understand where hand-offs between teams occur How: Map critical path of processes where bottlenecks and blockers could occur. In addition, a RACI matrix mapped to individual's activities would demonstrate over - constrained roles and responsibilities.
41	Pay Processing	P0023	Automate Payroll Validation and Testing of Exceptions	This opportunity is directly related to Process and Technology / Automation. What: The Payroll validation process and Testing of exceptions within Employee Central Payroll is time consuming and need to be more efficient. Why: Currently, If there is a variance and something does not balance, then the Payroll validation process will need to re-run from the beginning instead of correcting the error and continuing with the process. How: Payroll module (SuccessFactors) should already investigate the exceptions and report the issues experienced during the testing phase in order to achieve a one-time-right process
42	Pay Processing	P0025	Review Management Approval for Personal Requests	This opportunity is directly related to Process and Technology / Automation. What: Approval of personal requests must often be managed manually Why: Time consuming and could be automated How: this could be managed through a workflow tool within ServiceNow

POL00401629

Opportunities Long List – People (9/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
43	Pay Processing	P0026	Review Personal Admin Changes (Benefits)	This opportunity is directly related to Process, Data and Technology / Automation. What: Changes to employees benefits details, e.g. pensions, the cycle to work scheme, involve lots of manual effort and dealing with the interfaces adds to the challenge.
44	Pay Processing	P0027	Improve Reconciliation of CFS Data for Payroll	This opportunity is directly related to Technology / Automation. What: Process requires manual intervention for reconciliation. Why: Incorrect/delayed/wrong entries leading to manual intervention; for example: correcting the entries, chasing people for inputs and responding to employee queries. How: Reconciliation of Core Finance System (CFS) data and processing of information through government portals with automated testing. Processing and reconciliation of report could be automated.
45	Pay Processing	P0028	Automated System Alerts for Absences & Stage Warning	This opportunity is directly related to Process and Technology / Automation. What: Lack of alerts currently generated for absences and overtime during the process. Why: Incorrect/delayed/wrong entries leading to manual intervention, for example: manually correcting the entries and chasing people for inputs. How: Automated systematic alerts generated from absences and overtime for stage warning prompts which could streamline the process.
46	Pay Processing	P0029	Review SuccessFactors Configuration for Replication Monitor	This opportunity is directly related to Process and Technology / Automation. What: Replication Monitor reviewed daily to correct errors, from inputting data wrong in SuccessFactors. Why: Why: A number of incidents continue to pop - up from employees who incorrectly input information into the system. How: Configuration review / automation of Replication Monitor alerts for relevant assignees to amend and update error in SuccessFactors
47	Pay Processing	P0031	Enable a notes page for the Payroll Team	This opportunity is directly related to Process and Technology / Automation. What: Pay Processing team are unclear on a number of inputs / entries by users when reviewing absences, overtime. Why: A number of cases require HRSC team members to reach out to the individual separately to confirm / review why inputs have been made. How: Confirm data entry points for the Pay Processing team to prevent back and forth with individual.
48	Pay Processing	P0034	Merge Expenses (Selenity) into One System	This opportunity links to Data and Technology / Automation. What: Currently, staff are logging their expenses on a third party tool (Selenity). Why: Third party applications are leveraged due to incorrect use of SuccessFactors. How: There is an opportunity for expenses to be input via payroll within the payroll system.

POL00401629

Opportunities Long List – People (10/10)

Count	Business Sub-Area	Unique ID	Opportunity	Description
49	Pay Processing	P0038	Central Management of Long term sickness / absence	This opportunity directly links to People & Process. What: When an employee is on long term sickness, maternity or other long term absence, line management can forget to follow or do not understand the necessary process. Why: This has led to pay inaccuracies for the individuals concerned. How: Bringing the management of these long term absences into the HRSC could reduce error and improve the employee experience.
50	Pay Processing	P0060	Optimise the Payroll & Pensions processing cycle	A review of the payroll & pensions processing cycle (which would incorporate the use of SF) will capture where efficiencies can be made from system and non system processes. A proposed time in motion analysis to deep-dive on the activities currently taking place
51	Rewards & Pension	P0054	Enhance Business Rewards Processes	This opportunity links to People and Process. What: Currently, HRSC and Rewards team face a number of hand-offs which are handled digitally and paper-based, without a clear documented process. Why: Identify possible process steps that could be automated utilizing existing systems How: Proposal to document key activities that occur within the reward plan process to prevent duplication of effort for the following year.

POL00401629

Deloitte Review - Quick Wins* – People (1/5)

Count	Business Area	Business Sub-Area	Unique Identifier	Opportunity Name	Description	Quick Win?	Shortlisted?
1	People	Advice Centre, Recruitment and Administration	P0002	Enable Employee Probation Alerting	This opportunity is directly related to Technology / Automation. What: Ability to provide alerting around probational end, with automated email sent to line management to ensure a compliant process. Auto-Escalation to HRBP after a set amount of time. Why: Lots of time spend within HRSCs on monitoring End of Probation and contract extensions. How: System to Proactively inform Line managers on their responsibility to follow up on contract updates	Y	
2	People	Advice Centre, Recruitment and Administration	P0004	Improve People Data Configuration	This opportunity is directly related to Process, People and Technology / Automation. What: Improve the existing People Data Configuration in SuccessFactors Employee Central (Core HR). Why: Due to incorrect configuration and/or outdated foundation tables the system is automatically prompting incorrect data based on Data Changes that need to be corrected by HR Admin after completing the request. How: Currently a number of SF design improvements for example:- Upload of current rate tables - FTA contract (10 hour) leading to automatic input of incorrect inner / outer London waiting allowance - System alert for incorrect data input - automatic pro-rate salary - Salary set up e.g. £20,000 set up at £19,997.	Y	Y
3	People	Advice Centre, Recruitment and Administration	P0050	Install a Pool Laptop for Supply Chain Staff	This opportunity links directly to People. What: Post Office staff (deport staff) face difficulties accessing technology platforms where a number of issues / enquires could be answered. How: Where availability to laptops might be limited, installation of a pool laptop at each of the locations so employees are able to log into SuccessFactors would alleviate a number of incidents that are picked up by the HRSC. For instance, incorrect overtime hours, sick pay, absences etc.	Y	
4	People	Advice Centre, Recruitment and Administration	P0051	Prevent / Stop Calls to the Advice Centre	The opportunity links to People & Process. What: Currently, a percentage of staff are spending their time reviewing phone call enquires, with sufficiently large volumes monthly. Why: Typically, the business refer staff to policies that are available to read on the PeopleHub. A sufficient amount of time is spent explaining content, where it can be accessed through digital tools. How: By stopping calls, this will introduce a self-service mind-set across the business.	Y	
5	Finance	FA&G	F0109	Automate the fixed asset sweep process to reduce manual excel process in order to reduce time at period close	This opportunity relates to technology and process. It is regarding the monthly process of fixed asset sweep. At the moment this is really manual and done mostly on Excel. There is potential for VBA / Macro solution (although PO tends to discourage these solutions as they are hard to maintain due to the capability not being widespread). Could also explore whether use of SAP could be maximised for this process - so there is less or no reliance on Excel and it is all done in system.	Y	

***Quick Win assessment by project team**; criteria to determine a "Quick Win" is that the opportunity requires either minimal or none of the following: system update/ new functionality to be purchased, wider organisation change, significant investment. A "Quick Win" can be implemented or delivered in < 3 months.
** Benefit only available for shortlisted items

POL00401629

Quick Wins* – People (2/5)

Count	Business Area	Business Sub-Area	Unique Identifier	Opportunity Name	Description	Quick Win?	Shortlisted?
5	People	Advice Centre, Recruitment and Administration	P0036	Connect Job Level to Base Compensation (Non - Management)	This opportunity links to Data and Technology / Automation. What: When assignment of job level in recruitment / administrative changes, there is a lack of, or incorrect connection between job level and base salary. This directly effects all non-management staff. Why: There is a manual pro-rata for salary and holiday. How: Amend SuccessFactors to allow for change to the base salary each year, which can then be automatically updated for new and existing employees.	Y	
6	People	Advice Centre, Recruitment and Administration	P0044	Automation of Pay Progression Process	This opportunity is directly related to Process & Technology / Automation. What: Currently, salary progressions are done manually, with no automatic configuration. Why: The team on the ground is currently running an excel analysis, checking who require a salary progression, sending an email to the manager to confirm and make the adjustment. Upon completion, a letter of agreement is shared with the individual which is completed manually. How: Automation of pay progression based on automated alert raised to the team for individual close to their probation / scheduled date, to process pay progression case.	Y	
7	People	Change and Integration	P0049	Automation of Leavers Termination Date	This Opportunity links to Technology / Automation. What: Currently, there are number of multiple screens in SuccessFactors that need to be updated with the termination date - this has to be manually updated. Why: For instance, if the leaver had a company card, the team would require an input of the end date in SuccessFactors. How: The termination date does not pull throughout the entire system.	Y	
8	People	HR Systems & MI	P0001	Optimise System Role Based Permissions	This opportunity is directly related to Process and Technology / Automation. What: Optimise the role based permissions in SuccessFactors for all roles within the HRSC. Why: Lots of processes (for e.g.. Pay Related) require involvement from different HRSC Team members with different permissions. This is reducing the turn around time per process. How: Focus on trust-based elements by giving administrators access to the full dataset of Job/Comp Information covering their workflows in 1 step.	Y	Y

*__Quick Win assessment by project team__; criteria to determine a "Quick Win" is that the opportunity requires either minimal or none of the following: system update/ new functionality to be purchased, wider organisation change, significant investment. A "Quick Win" can be implemented or delivered in < 3 months.
** Benefit only available for shortlisted items

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Quick Wins* – People (3/5)

Count	Business Area	Business Sub-Area	Unique Identifier	Opportunity Name	Description	Quick Win?	Shortlisted?
9	People	HR Systems & MI	P0021	Innovate HR/IT Systems Forum	This opportunity is directly related to People & Process. What: Review the Change Approval Board (CAB) Governance and outline the process for required system changes. Streamline the forums and review required attendees. Why: Particular need for greater and earlier involvement from key business stakeholders feeding in the requirements for change within SuccessFactors. How: Which stakeholders are currently involved in the Change Request process; which stakeholders should be included in the To-Be State (Clear representation from Business HR) and how often are SuccessFactors Release Updates shared throughout this community	Y	Y
10	People	HR Systems & MI	P0020	Review Accenture Roadmap & AMS Contract	This opportunity is directly related to People & Process. What: The Governance Model on HR IT (SuccessFactors) support must be revised. Contractual decisions on RACI between Post Office People, IT and Accenture to be clarified. Why: Current support contract with Accenture disallows the Post Office team to be self-driving and is causing significant delays in resolving defects and processing change requests not fulfilling the current HR Business requirements which negatively impacts the user experience throughout the HR Community How: Review current Governance Model and identify opportunities for improvement towards current contract and setup of SuccessFactors	Y	Y
11	People	HR Systems & MI	P0014	Development of System Knowledge Capabilities	This opportunity is directly related to People. What: Improve SuccessFactors and Reporting knowledge capabilities within the HR Systems and MI Team. Why: Building a knowledge network within the Post Office will reduce the dependency on Vendor capability and will create efficiencies and self-driving teams in terms of System defect management, change request optimisation and Report Creation How: Greater access to be granted in the Development system in order to execute more tasks independently of the AMS vendor. Leverage the SAP knowledge Portals; Identify need for SuccessFactors Certification training.	Y	Y
12	People	HR Systems & MI	P0040	Alignment of SuccessFactors Release to Business Needs	This opportunity links to Technology / Automation and Process. What: Currently, SuccessFactors release notes are not translated from technical language into business language, therefore, opportunities to improve user experience within system design is missed. Why: Current vendor outlines the Release Updates solely on technical impact without translating this to the business impact. Within PO HR System Team there should be capabilities to add this perspective and share into a wider business group (possibly to be formed) How: Review SuccessFactors (bi - annually) release cycle and align towards business needs and requirements, to address where these can be met. This could be explored in CAB forums led by the SuccessFactors HRSC team.	Y	

*__Quick Win assessment by project team__; criteria to determine a "Quick Win" is that the opportunity requires either minimal or none of the following: system update/ new functionality to be purchased, wider organisation change, significant investment. A "Quick Win" can be implemented or delivered in < 3 months.
** Benefit only available for shortlisted items

POL00401629

Quick Wins* – People (4/5)

Count	Business Area	Business Sub-Area	Unique Identifier	Opportunity Name	Description	Quick Win?	Shortlisted?
13	People	HR Systems & MI	P0032	Review of SucessFactors System Notifications	This opportunity links directly to Data and Technology / Automation. What: A number of system notifications could be leveraged to support line management with a number of their responsibilities, send notifications where action is needed. Why: HRSC are having to complete a number of re-work activities on a number of cases where line management have not completed the task. How: Audit / review all SuccessFactors notifications sent out from the system to identify where: A) link to pages on PeopleHub. B)Improve quality, clarity and timing of the message – which includes any escalated notifications to i.e. second line manager or HRBP. An example of a good automated notification which would help (particularly Luke in HRSC) would be a weekly automated email which is sent to a line manager when a direct report has a live sick absence on the system reminding them (just in case they haven't closed the absence on SF) and highlighting things like PeopleHub / OH assist for referrals and the Sick Absence Policy.	Y	
14	People	HR Systems & MI	P0012	Optimise Organisational Restructure Process	This opportunity is directly related to Process and Technology / Automation. What: Optimise the Organisational Restructure Process by enabling mass changes to Organisation & People Data Why: The recent reorganisation requires mass data changes to be made in the system to individuals' divisions and departments. This is a manual task, requiring each individual's profile to be updated one by one. The foundation data to be updated with help of Accenture due to wide-reaching impacts and necessary changes to resolve issues, e.g. for RBPs and workflows. How: Opportunity to identify the functionality of mass data changes for Foundation and People Data within SuccessFactors	Y	
15	People	HR Systems & MI	P0011	Automation of Settlement Agreement Packs	This opportunity is directly related to Process and Technology / Automation. Pre-requisite to the opportunity below is captured in [P0046]. What: Automation of Settlement Agreement Packs Why: A lot of time is currently spent on processing the information for the pack as information is pulled from SuccessFactors and then manual calculations are performed. In addition, there is an opportunity to automate signatory acceptance. This is currently paper based and it takes full days to put together the settlement agreement packs. How: Achieve automation including the mail merge of document packs and electronically sending documents (statutory agreements) to individuals and to legal counsel.	Y	
16	People	HRSC	P0057	Review HRSC and POL Roles and Responsibilities	This opportunity links to People and Process. What: Perform a review of HRSC and Post Office business stakeholders key roles and responsibilities where there are inter-dependencies. Why: This is to understand where hand-offs between teams occur How: Map critical path of processes where bottlenecks and blockers could occur. In addition, a RACI matrix mapped to individual's activities would demonstrate over - constrained roles and responsibilities.	Y	Y

***Quick Win assessment by project team**; criteria to determine a "Quick Win" is that the opportunity requires either minimal or none of the following: system update/ new functionality to be purchased, wider organisation change, significant investment. A "Quick Win" can be implemented or delivered in < 3 months.
** Benefit only available for shortlisted items

POL00401629

Quick Wins* – People (5/5)

Count	Business Area	Business Sub-Area	Unique Identifier	Opportunity Name	Description	Quick Win?	Shortlisted?
17	People	Pay Processing	P0028	Automated System Alerts for Absences & Stage Warning Leveraging a Centralised Tool	This opportunity is directly related to Process and Technology / Automation. What: Lack of alerts currently generated for absences and overtime during the process. When an employee is on long term sickness, maternity or other long term absence, line management can forget to follow or do not understand the necessary process. Why: Incorrect/delayed/wrong entries leading to manual intervention, for example: manually correcting the entries and chasing people for inputs. This has led to pay inaccuracies for the individuals concerned. How: Automated systematic alerts generated from absences and overtime for stage warning prompts which could streamline the process. By also, bringing the management of these long term absences into the HRSC could reduce error and improve the employee experience.	Y	Y
18	People	Pay Processing	P0023	Automate Payroll Validation and Testing of Exceptions	This opportunity is directly related to Process and Technology / Automation. What: The Payroll validation process and Testing of exceptions within Employee Central Payroll is time consuming and need to be more efficient. Why: Currently, If there is a variance and something does not balance, then the Payroll validation process will need to re-run from the beginning instead of correcting the error and continuing with the process. How: Payroll module (SuccessFactors) should already investigate the exceptions and report the issues experienced during the testing phase in order to achieve a one-time-right process	Y	
19	People	Pay Processing	P0031	Enable a notes page for the Payroll Team	This opportunity is directly related to Process and Technology / Automation. What: Pay Processing team are unclear on a number of inputs / entries by users when reviewing absences, overtime. Why: A number of cases require HRSC delegates to reach out to the individual separately to confirm / review why inputs have been made. How: Confirm data entry points for the Pay Processing team to prevent back and forth with individual.	Y	
20	People	Pay Processing	P0025	Review Management Approval for Personal Requests	This opportunity is directly related to Process and Technology / Automation. What: Approval of personal requests must often be managed manually Why: Time consuming and could be automated How: this could be managed through a workflow tool within ServiceNow	Y	
21	People	Rewards and Pension	P0054	Enhance Business Rewards Processes	This opportunity links to People and Process. What: Currently, HRSC and Rewards team face a number of hand-offs which are handled digitally and paper-based, without a clear documented process. Why: Identify possible process steps that could be automated utilizing existing systems How: Proposal to document key activities that occur within the reward plan process to prevent duplication of effort for the following year.	Y	

***Quick Win assessment by project team**; criteria to determine a "Quick Win" is that the opportunity requires either minimal or none of the following: system update/ new functionality to be purchased, wider organisation change, significant investment. A "Quick Win" can be implemented or delivered in < 3 months.
** Benefit only available for shortlisted items

POL00401629

Policy *Procurement Policy*

Version – V0.6 September 2020

DRAFT

12

POL00401629

1. Overview 4
1.1. Introduction by the Policy Owner 4
1.2. Purpose 4
1.3. Core Principles 4
1.4. Application 5
1.5. The Risk 6
1.6. Legislation 6
1.7. Industry Guidance 6
2. Risk Appetite and Minimum Control Standards 9
2.1. Risk Appetite 9
2.2. Policy Framework 9
2.3. Who must comply? 9
2.4. Roles & Responsibilities 10
2.5. Minimum Control Standards 12
3. Definitions 14
3.1. Tools 14
3.2. Definitions 14
4. Where to go for help 15
4.1. Additional Policies 15
4.2. Supporting Processes and Documentation 15
4.3. How to raise a concern 15
4.4. Who to contact for more information 16
5. Governance 17
5.1. Governance Responsibilities 17
6. Control 18
6.1. Policy Version 18
6.2. Policy Approval 18
Company Details 18

DRAFT

[1]In this Policy "Post Office" means Post Office Limited and "Group" and shall include Post Office Management Services Limited and Payzone?.

[2]In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants [and anyone else working for or on behalf of Post Office (save for third party suppliers and their personnel).

12

POL00401629

DRAFT

POL00401629

1. Overview

1.1. Introduction by the Policy Owner

The Procurement Director has overall accountability to the Board of Directors for the governance and implementation of controls applied to procurement activities for goods and services. The Procurement Policy and its associated processes and controls are an agenda item for the Audit and Risk Committee and the Post Office Board is updated as required.

Post Office spends approximately £500m per annum on goods and services from third parties. From an operational and commercial perspective, the management of this expenditure is critical in achieving commercial sustainability within the legal framework set out for public procurement with which Post Office Ltd must comply.

The Policy sets out the manner in which the Post Office will govern the procurement activities for goods and services. It covers processes in which the Procurement teams with cross functional stakeholders identify, qualify and engage a strong supplier base, ensuring compliance and reliable supply.

This Policy should be read in conjunction with related policies setting out the processes in which the organisation sources and selects and contracts with its suppliers, executes the purchasing processes through defined and controlled purchasing channels, and commercially and operationally manages the services on an ongoing basis (see links to associated policies and processes in Appendix C)

1.2. Purpose

The purpose of this policy is to set out the way in which the Post Office will govern the procurement activities for goods and services including the selection of suppliers and the sourcing and procurement exercises.

It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

For definitions please see section 3.1.

1.3. Core Principles

Procurement is the act of obtaining goods or services, typically for business purposes. Sourcing is the process of defining the required goods and services, the execution of tender or bid process and, the evaluation of responses, selection and appointment process for the preferred bidder. .

The over-riding procurement policy requirement is that all public procurement must be based on value for money, defined as "the best mix of quality and effectiveness for the least outlay over the period of use of the goods or services bought". This should be achieved through competition There are limited exemptions to when a competition is not required, these set out within the legal framework. Public authorities can award on the basis of: (i) price or cost alone (taking into account cost effectiveness); (ii) fix the price and just evaluate on quality; or (iii) a combination of these two options. Provided the basis on

DRAFT

POL00401629

which a commercial response shall be evaluated is communicated clearly, in advance of bid submissions and fully adhered to, this is compliant.

Public sector procurement is subject to a legal framework which encourages free and open competition and value for money, in line with EU and domestic law and EU and UK Government guidance. There is also law and guidance to support growth by improving SME access to public contracts, particularly for low value contracts. This may require the advertisement of public contract opportunities and the publication of contract awards.

Procurement at Post Office shall be driven by the following Guiding Principles in all procurement activities:

Cost

- Achieve sustained value by progressively managing POL's expenditure, maximising value and seeking continuous improvement and innovation for the Post Office.

Contract

- Reduce operational, commercial, reputational and legal risk to the Post Office by ensuring contracts which are fit for purpose are in place to ensure the delivery of goods and services to the agreed requirements, to seek continuous improvement from the commercial relationship agreements, and with appropriate levels of control and oversight as relevant to the goods and service supplied.

Compliance

- To ensure that procurement activity carried out within the Post Office complies with the relevant regulations in respect of public sector procurement, EU and UK guidance,and in accordance with Post Office governance and risk management.
- Compliance to internal Post office Group policy on consultation with key stakeholders ensuring they have been advised of, consulted and approved where appropriate in line in advance of and during a procurement process. Key Stakeholders may include Compliance [Data Protection, Regulatory, Financial Crime], Information Security, Legal, Business Continuity, Corporate Responsibility, HR and Finance;

Consolidation

- Deliver efficiencies to Post Office by managing the supply base to consolidate spend with onboarded strategic suppliers, and to optimise the total number of suppliers and contracts requiring direct management.

1.4. Application

This Policy is applicable to Post Office Ltd and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Post Office's Risk Appetite.

The risk to the Group from Procurement is reviewed by the board annually.

In exceptional circumstances, where the procurement activity sits outside of the Post Office's accepted Risk Appetite a Procurement Risk Exception can be submitted for Board review and approval. For further information in relation to the risk exception process please contact the Risk & Assurance team.

DRAFT

POL00401629

1.5. The Risk

The Procurement Policy is designed to establish best practice and mitigate the risks which may arise during the course of a procurement. All procurement activities shall adhere to the Post Office Procurement Policy and the detailed guidance set out within the Post Office Legal Service Procurement Manual. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ Post Offices risk management principles.

Procurement activities shall be properly planned and carried out in a manner that will enhance Post Office's capability to prevent, withstand and recover from interruption to the supply of goods and services where commercially viable.

1.6. Legislation

The Post Office seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- Public Contract Regulation 2015,supporting UK Government guidance (referred to as Procurement Policy Notes) and EU law and guidance and case law
- Utilities Contracts Regulations 2016
- Competition Act 1998
- Concession Contracts Regulation 2016
- Modern Slavery Act 2015

1.7. Industry Guidance

Public Sector Procurement is subject to Public Contract Regulations ("PCR") 2015. PCR enables the public sector to focus on getting the right supplier in accordance with sound commercial practice. As a publicly funded organisation, compliance with PCRis mandated, insofar that it is relevant.

Procurement shall be driven by the Public Contract Regulations in all procurement activities. These are set out in detail within the Post Office Legal Services Procurement Manual and shall be updated from time to time in accordance with the law:

Supplier selection

- Selection and appointment of suppliers must be objectively and transparently based on their ability to perform as defined as well as taking into consideration social values, ethical practices and environmental impacts. In particular this includes confirmation of the acceptance of our Supplier Code of Conduct and financial due diligence. This will be managed through our on-boarding and sourcing procedures;
- Post Office staff do not enter into supplier selection, discussions with 3rd parties, make a commitment to spend, or undertake any procurement exercise without the involvement of the procurement team

Sourcing and Procurement exercises

DRAFT

POL00401629

- Must contract on the best possible terms for POL, managing the balance between opportunity & risk, and utilising existing contract provision where appropriate to comply with legislation, in particular Public Contract Regulations (2015);

- Ensure that transparency and accessibility is embedded within our processes and activities, so that equal opportunities for small and medium sized businesses, minority owned businesses, social enterprises and the voluntary and community sector will be provided in line with UK regulation;

- Ensure that the aims of the business on diversity, sustainability and other aspects of corporate social responsibility are embedded within our processes and activities

Managing Contractual Processes

- Manage the POL contracting process in accordance with internal governance and approval policy and process, and relevant external legislation,

- Ensuring that contracts are fit for purpose for the goods and services POL is contracting for. This includes defining vendor expectations, performance, scope of work, and deliverables. In particular, confirmation should be sought regarding understanding of and adherence to the following POL policies: Bribery and Corruption, Tax Evasion, Confidentiality and Health and Safety. All contracts must protect our physical and intellectual property and data and, in the interests of transparency, include a right of audit;

- Ensure a managed handover of agreements for contract management by the business using the Contract Management Framework, and any ongoing responsibilities for the resolution of issues raised in accordance with the contract.

- Post Office staff must not enter into any material contractual changes without the involvement of the procurement team, such as a change of scope or value outside of that which was originally advertised to the market in the procurement exercise.

Managing Suppliers

- Support Contract Managers in the business as they respond to performance issues and monitor suppliers, to ensure that the supply chain risk is managed and disputes are resolved.

- Ensure there is a defined governance structure in place to manage strategic and core suppliers so that there is a mechanism to escalate issues, to influence their priorities to align with ours, and to achieve a sustainable service through continuity planning.

- Periodically review the supply base with the relevant business unit to ensure that as services scale up, or down, appropriate supplier governance, commercial support and risk management is in place.

Managing Risk

- Understand the risks and complexities of the goods and services we procure to segment the supply base into tiers to identify the strategic, critical and core suppliers, and to conduct risk analysis on specific threats.

- Have contracts in place with suppliers that will mitigate risk and enable the monitoring of improvement over time.

POL00401629

- Work with Contract Managers to ensure that the business has adequate arrangements in place with critical suppliers for supply disruption, business continuity and disaster recovery.

DRAFT

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Post Office will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Post Office is willing and able to tolerate.

The Post Office takes its legal and regulatory responsibilities seriously and consequently has:

- Tolerant risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- Averse risk appetite for litigation in relation to high profile cases/issues
- Averse risk appetite for litigation in relation to Financial Services matters
- Averse risk appetite for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the Group
- Averse Risk Appetite in relation to unethical behaviour by our staff.

Therefore, for the purposes of clarity, the risk appetite for Procurement non compliance to Public Contract Regulations is Averse, except in those limited circumstances where there are *significant* conflicting imperatives between conformance and commercial practicality.

Commented [BB1]: Risk have requested a statement to set out the specific appetite for procurement risk.

In this situation, a risk exception waiver will be required. This process is set out within the Procurement Risk Exception Process 2020 set out within Appendix B.

2.2. Policy Framework

Post Office has established a suite of Procurement policies and procedures, on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to assist with Supplier Management, Contractual Processes, and Procurement exercises these have been developed to comply with applicable legislation and regulation.

2.3. Who must comply?

This policy applies to all employees who procure goods and service from external suppliers. Compliance with this policy is mandatory for all business units within Post Office Ltd [POL]. Other Group entities [Post Office Insurance and Payzone] operate under separate Procurement Policies as they are not subject to Public Contract Regulations. Supporting processes must be complied with by these Group entities where clearly stated.

In the case of agencies and consultancies, all contracted personnel working on behalf of POL shall be made aware of this policy and shall comply with all procurement procedures listed within the Procurement department guidance.

All employees who procure from suppliers should work to our values Care, Challenge and Commit and our standards set out in the Code of Business Standards and the other POL

DRAFT

POL00401629

policies listed in 4.1.

This policy does not apply directly to outsourced service providers or to suppliers; however, suppliers are required to comply with our Supplier Code of Conduct which seeks to ensure our outsourced service providers and suppliers must: support the governance of POL; mitigate the risks faced by POL; and support the quality of service we provide to our customers, our policies and other legal requirements (including finance, health and safety, human rights and labour standards, and employment laws);

Where non-compliance is identified the matter must be referred to the Procurement Director, Director of Risk, Compliance Director and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

2.4. Roles & Responsibilities

Procurement shall drive the procurement process, negotiate commercial arrangements, and support the means by which procured solutions are delivered.

Procurement Director is responsible for:

- Administering this policy on behalf of the CEO
- Developing and rolling out the supporting strategies to drive continual performance improvement.

Procurement Department is responsible for:

- Driving, adopting and sharing best practice procurement and sourcing standards and initiatives;
- Developing category strategies and driving the optimisation of the supply base and best value for POL
- Creating compliant procurements exercises and contracts with adequate contract handover to Contract/ Vendor Managers to deliver
- Developing and mutually beneficial collaborative trading relationships with suppliers;
- Monitoring the evaluation and assessment of suppliers' supply practices (including ethical, sustainable measures), taking appropriate commercial action as necessary.

Contract/ Vendor Managers are responsible for:

- Monitoring the evaluation and assessment of suppliers' supply practices (including ethical, sustainable measures),
- Take appropriate commercial action and escalating as necessary as set out within the Contract Management Framework.

Directorate/Business Managing Directors are responsible for:

- Ensuring that this policy, supporting procedures and corrective actions are implemented and complied with;
- Ensuring all key stakeholders have been advised of, and consulted where appropriate in line with internal governance in advance of and during a procurement process. Key Stakeholders may include Compliance, Information Security, Legal, Data Protection, Business Continuity, HR and Finance; and
- Leading by example in protecting the POL brand and championing knowledge sharing across the divisions.

DRAFT

POL00401629

Managers are responsible for:

- Implementing and enforcing the processes and procedures;
- Ensuring that their people are aware of their responsibilities and receive appropriate training.

Suppliers are responsible for:

- Acting in accordance with this policy and associated procedures and guidance provided in their contracts and the Supplier Code of Conduct.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

DRAFT

POL00401629

2.5. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Activities of employees and consultants	Failure to ensure that Consultants and Employees comply with the Post Office Procurement Policy and supporting procedures	**Preventative Control** All procurement activities shall adhere to the Post Office Procurement Policy. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ POLs risk management principles.	Procurement Director	Ongoing
Procurement activity	Failure to uphold good practise procurement principles	Procurement activities shall be properly planned and carried out in a manner that will enhance POL's capability to prevent, withstand and recover from interruption to the supply of goods and services where commercially viable.	Procurement Team	Ongoing
Data Input	Maintenance of accurate data input within the eProcurement systems to monitor compliance.	Compliance shall be collated periodically using spend and sourcing analytics extracted from POLs eSourcing and eProcurement systems, the Risk Committee reporting, and issues reported by the relevant category leads and line managers. It shall be the responsibility of the line managers to deal with the instances of non-compliance within their category teams and raise any disciplinary actions	Procurement Managers	Ongoing

DRAFT

POL00401629

Conflict of Interest	Failure to manage conflicts of interest related procurement	**Preventative Control** During procurement activity, conflicts of interest declarations are issued and reviewed. Any conflicts of interest risks are mitigated and recorded. Suppliers are contracted to comply with anti-bribery and corruption laws.	Procurement Director	Ongoing
Supplier Conduct	Reputational and commercial risk from poor supplier conduct	Effective due diligence of the supply base with additional risk-based assessments and monitoring against Supplier Code of Conduct	Procurement Team	Ongoing
Vulnerable Customers	Customers not being able to access our branches, products or services.	During the tendering application the needs of vulnerable customers should be considered at the start of the process. This is captured via in-depth supplier questionnaires and supporting documentation.	Procurement Team	Ongoing

DRAFT

POL00401629

3. Definitions

3.1. Tools

1. **Web3** Source to Settle system - Sourcing and Contract Management through to Purchase to Pay modules
2. **Contracts Finder** – government portal used to publish opportunities to potential suppliers and/or notices of award to the winning bidders

3.2. Definitions

1. **POL** – Post Office Limited entities and subsidiaries
2. **Post Office Insurance** – the Post Office Insurance business which is separate from the POL in regard to public subsidy.
3. **PCR** – Public Contract Regulations 2015 are rules on the procedures for procurement by contracting authorities with respect to public contracts.
4. **FCA** - Financial Conduct Authority regulates how insurance firms behave, as well as more broadly the integrity of the UK's financial markets
5. **Material contractual change** – change of scope/ value outside what it was advertised for.

DRAFT

POL00401629

4. Where to go for help

4.1. Additional Policies

This Policy is one of a set of Post Office policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2. Supporting Processes and Documentation

Public Procurement is subject to extensive regulation and guidance in the manner in which opportunities are advertised, tendered for, evaluated and awarded.

A full set of up to date documentation is available via the Procurement Intranet site and a list of key supporting guidance documents and interdependent policy and processes are set out below. Documents marked with an asterix form appendices to this Policy.

4.2.1. Post Office Legal Services Procurement Manual

4.2.2. Post Office Guidance on UK Regulations on Sub Threshold Contracts 2020*

4.2.3. Procurement Risk Exception Process 2020*

4.2.4. PP2 Purchasing Process V0.1 2020*

4.2.5. Supplier Onboarding Process

4.2.6. Contract Management Framework Policy [September 2020]

4.2.7. Contract Execution Policy [September 2020]

4.3. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to report without any undue delay.

Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: [redacted] or by telephone on: [redacted].
- The confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on [redacted], or
- Via a secure on-line web portal: http://postoffice.ethicspoint.com/

DRAFT

POL00401629

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Correspondence Team.

4.4. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Procurement Director.

DRAFT

POL00401629

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the Procurement Director, Post Office Limited.

The Policy owner is the Procurement Director who is responsible for ensuring that the Procurement Department conducts an annual review of this Policy and tests compliance across the Group. Additionally, the Procurement Director and the Procurement Department are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

Appendix A

Post Office Guidance on UK Regulations on Sub Threshold Contracts 2020

Appendix B

Procurement Risk Exception Process 2020

Appendix C

PP2 Purchasing Process V0.1 2020

DRAFT

POL00401629

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
	0.1		Draft Version
09/06/2020	0.2	Susan Godfrey	Draft Version
08/09/2020	0.5	Barbara Brannon	Reviewed and incorporated feedback from Legal and Compliance teams.

6.2. Policy Approval

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

Committee	Date Approved
POL R&CC	
POL ARC	

Policy Sponsor: [*name of policy sponsor*]
Policy Owner: Procurement Director
Policy Author: Procurement Performance & Operations Manager

Next review: [*date of next review in DD MM YYYY format*]

DRAFT

Company Details

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

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

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

POL00401629

DRAFT

Procurement Policy

Appendix A

Guidance on Sub Threshold Awards

Version – V0.1

12

POL00401629

1. Overview 3
1.1. Purpose of this guidance 3
1.2. Core Principles 3
1.3. Application 3
1.4. The Risk 4
1.5. Post Office policy on Sub Threshold Procurement 4
1.5.1. Awards under £25k 4
1.5.2. Awards between £25k and the PCR threshold* 4
1.6. Industry Guidance 5

[1] In this Policy "Post Office" and "Group" means Post Office Limited, Post Office Management Services Li[1]mited and Payzone Bill Payments Limited.

[2]In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

DRAFT

12

[1]

POL00401629

1. Overview

1.1. Purpose of this guidance

This guidance has been established to set the minimum operating standards relating to the risk management of procurement activity under PCR threshold values. These thresholds are updated every two years to account for exchange rate variations between the UK and the Eurozone. throughout the Post Office Ltd.It forms an appendix to the Post Office Ltd Procurement Policy 2020.

1.2. Core Principles

Since the 1970s, the EU has adopted legislation to ensure that the EU public procurement market is open and competitive and that suppliers are treated equally and fairly. The rules cover aspects such as advertising of contracts, procedures for assessing company credentials, awarding the contracts and remedies (penalties) when these rules are breached.

The EU rules are contained in a series of directives that are updated from time to time. Member states have to make national legislation (regulations) to implement the EU rules in domestic law by certain deadlines. The most recent update of the EU procurement directives was in April 2014.

- EU Public Contracts Directive 2014;
- Public Contracts Regulations 2015;
- The EC treaty principles underpin the EU law;
- There is also a substantial body of EU and UK case law on the application of the directive and regulations;
- EU and UK government guidance (including PPNs from Cabinet Office).

This policy identifies the key practical issues that feature in below threshold procurements including the need to advertise, the impact of the Treaty on the Functioning of the European Union [TFEU] on the award of contracts and the risks of not observing the rules.

1.3. Application

This guidance is applicable to all areas within the Post Office Ltd and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Post Office Ltd's's Risk Appetite. This guidance will be reviewed annually in line with the Procurement Policy it forms part of.

In exceptional circumstances, where risk sits outside of the Post Office Ltd's accepted Risk Appetite a Procurement Risk Exception can be raised and submitted to Board for review and approval.

For the avoidance of doubt, all Procurement Risk Exceptions of any value will be referred to Board.

For further information in relation to the risk exception process please contact Procurement and the Risk & Assurance team.

POL00401629

1.4. The Risk

The principles set out in the TFEU (Treaty Principles) will generally apply to all actions of a contracting authority except where there is no cross border interest.

This appendix sets out the key controls and guidance in relation to Sub-threshold procurements for Supply and Services contracts only. Please consult with Procurement if contemplating any other contract set out within 1.6 "OJEU Thresholds".

1.5. Post Office policy on Sub Threshold Procurement

Detailed legal guidance on Sub Threshold Procurement is set out within 1.6 of this document.

1.5.1. Awards under £25k

a) Awards under £25k may be made without a competitive process subject to Procurement view that Cross Border interest does not apply. Such awards must be one off in nature and not be for recurring goods and services.

b) "Slicing and dicing" of awards for the purposes of staying under this threshold is against the law.

c) Where the ongoing requirement is unknown at the point of award, it should be assumed that a competitive process will be required for any subsequent extensions or contracts, where the cumulative value will breach £25k.

d) Business units should therefore consider whether it is more expedient to run a competitive process from the outset to reduce the risk of business or project disruption.

e) Business units should consult with Procurement as to whether the use of a Corporate Purchasing Card is a more efficient route to market.

f) Contracts must be executed on Post Office terms and conditions and payment terms may not be varied without written approval from a Finance Director.

g) No financial or contractual commitment may be made to the supplier until a contract has been executed in line with Post Office Contract Execution Policy.

h) Where the opportunity is deemed to be of cross border interest, the opportunity must be advertised on Contracts Finder and a transparent procurement process must be run.

1.5.2. Awards between £25k and the PCR threshold*

Please note:

Breaches of this policy will be investigated and may result in referral to HR.

All breaches will be treated as a Procurement Risk Exception and will be reviewed by Board.

POL00401629

In making a sub threshold award to a third party between £25k and £189,330 the following **Post Office policy** applies:

a) All awards will be presumed to have cross border interest without a Legal Risk Note [LRN] to support UK only interest.

b) The opportunity must be publicly advertised on Contracts Finder.

c) A competitive process must be run.

d) Notice of the award must be published in a timely way.

Where it is argued that there is no cross border interest:

a) Procurement, with business unit support will examine and prepare a briefing note for Legal in respect of any LRN,

b) The business unit must bear the cost of preparing the Legal Risk Note.

c) A competitive process should be run, [but is not mandatory]where time permits in order to facilitate better value for money, enhanced service offerings and better terms and conditions.

Awards which do not comply with these principles will be treated as a Procurement Risk Exception and will be subject to Board oversight.

Please also note the same principles apply for awards >£25k:

a) "Slicing and dicing" of awards for the purposes of staying under this threshold is against the law.

b) Where the ongoing requirement is unknown at the point of award, it should be assumed that a competitive process will be required for any subsequent extensions or contracts, where the cumulative value will breach the upper threshold over the term of the contract.

c) Business units should therefore consider whether it is more expedient to run a compliant above threshold process from the outset to

   a. reduce the risk of business or project disruption where a change in provider may result in a requirement to transfer knowledge, skills and loss of acquired knowledge.

   b. Build in financial contingency for delays, additional requirement and resourcing.

Commented [BB1]: This is the proposed policy. For discussion at GE/ARC

Commented [BB2]: This is risk averse but the alternative is to go straight to LRN on all minor procurements?

Commented [BB3]: Placeholder for discussion

Commented [BB4]: Note that this is proposed internal policy but is not a legal requirement.

DRAFT

12

1.6. Industry Guidance

FN1 – What is a below threshold contract?

1. **OJEU Thresholds**

POL00401629

Below threshold contracts are those contracts which are valued **below** the OJEU thresholds. The OJEU thresholds are currently:

(a) Works £4,733,252

(b) Supply and Service Contracts (sub-central authorities) £189,330

(c) Light Touch Regime £663,540

(d) Concession Contracts £4,733,252

2. **Is procurement law concerned with below threshold contracts?**

Yes. When placing below threshold public works, services, supplies or concessions contracts POL must comply with:

(a) Treaty Principles[2] where contracts attract Cross Border interest.[3]

(b) the Public Contracts Regulations 2015 (the **Regulations**) which impose obligations on POL when awarding contracts which are ≥£25k.[4]

(c) any internal guidance, to the extent applicable.[5]

FN2 – Rules on accumulation

When assessing whether an OJEU threshold has been met, POL should have regard to the rules on accumulation of contracts. These are contained in regulation 6 of the Regulations. These can require POL to accumulate the value of multiple contracts when assessing whether the OJEU threshold has been met. For example, the value of regular purchases made over a period of 12 month should be accumulated for the purposes of calculating whether the values of such contracts meet the OJEU threshold.

A contract can in isolation appear to be below threshold, however, when the rules on accumulation are applied, it and related contracts may need to be treated as above OJEU threshold contracts.

FN3 – Does a contract have cross border interest?

1. **What is cross border interest?**

A contract will have cross border interest if it is of interest to suppliers located in other EU Member States (this includes suppliers which are UK subsidiaries of EU companies).

2. **How do we know if a contract has cross border interest?**

This is an objective test.[6] The key question is

Would the realistic hypothetical European bidder have bid for the contract had the opportunity arisen?

[2] See for example *Bent Mousten Vestergaard* (C-59/00), *Serrantoni* (C-376/08), *SECAP* (C-147/06)

[3] See FN 3

[4] See FN 6

[5] See FN 5

[6] *Ocean Outdoor UK Limited v London Borough of Hammersmith and Fulham* [2018] EWHC 2508 (TCC)

POL00401629

There is no definitive list of factors to be taken into account when considering whether there is cross border interest. However POL should at least consider the following:

(a) value of the contract;

(b) location of the works/services/supplies;

(c) the technical nature of the contract and the specific characteristics including whether the particular services/works/supplies are being provided in other Member States or are UK specific?[7];

(d) whether the opportunity is strategic such that a new entrant from another Member State would pursue the opportunity for strategic business purposes (e.g. to "establish itself on the market of that State and to make itself known there with a view to preparing its future expansion"[8]); and

(e) whether any interest has been expressed by suppliers from other Member States (including UK subsidiaries of European companies) and (in retrospect) whether any complaints have been made by operators situated in other Member States.[9]

3. **What about low value contracts?**

There is a presumption that very low value contracts are unlikely to attract cross border interest.[10] However, it remains possible that cross border interest could be found in contracts of low value (<£25k), where the other factors support EU interest.[11] Therefore when placing low value contracts POL must still conduct an assessment as to whether cross border interest is present. If cross border interest is present, a procurement process which complies with the Treaty Principles is required. This will include suitable advertisement of both the contract opportunity and the contract award.[12] Regardless of whether cross border interest is present, POL must adhere to any internal rules, to the extent applicable.

4. **What about light touch regime contracts?**

The light-touch regime is a specific set of rules for certain service contracts that tend to be of lower interest to cross-border competition (e.g. postal services). There is a presumption that below threshold light touch contracts will **not** have cross border interest. Therefore cross border interest would likely only be present in below threshold light touch regime contracts in exceptional circumstances.[13]

FN4 – Could POL test cross border interest, if unsure?

[7] Oftalma Hospital Srl v Commissione Istituti Ospitalieri Valdesi (CIOV),

[8] *Comune di Ancona*, C-388/12

[9] *Tecnoedi Costruzioni*,C-318/15

[10] SIGMA "Brief 15: Below Threshold Contracts"

[11] *SECAP and Santorso*, C-147/06 and C-148/06

[12] Case law and statutory guidance are silent on whether contract award information must be published for <£25k contracts which attract cross border interest. The risk adverse approach is to assume publication is required.

[13] See recital 117 of Directive 2014/24/EU

POL00401629

If, having assessed the relevant factors, POL remains unsure as to whether there is cross border interest in a particular opportunity, the "no procurement law risk" option would be to assume that there is cross border interest.[14]

However, the need to rely on the assumption could potentially be reduced where POL is able to gather additional information from the market. There are various methods to test the market. The greatest level of certainty could be gained by POL issuing a PIN on the Official Journal, seeking very general expressions of interest. However, softer testing, for example by contacting non UK suppliers or hosting an advertised Suppliers' Day may also generate some relevant intelligence. POL would of course need to determine whether such market engagement was otherwise considered appropriate.

FN5 – Requirement to adhere to any POL procurement policy (to the extent applicable)

As at the date on which this guide has been produced, we are advised that POL does not operate a formal procurement policy. However, to the extent that this is developed in the future, this should be adhered to for contracts of all values.

FN6 – How to procure in compliance with the Treaty Principles

As above, POL will be required to comply with Treaty Principles if placing below threshold public services, works, supplies or concessions contract which attract cross border interest.

5. **What are the relevant Treaty Principles?**

   Of particular importance are the principles of equal treatment, proportionality, non-discrimination on grounds of nationality and transparency.[15]

6. **What are the implications for POL's below threshold procurements?**

   Where the Treaty Principles apply, there must be some form of open competition for below threshold contracts which complies with the following:

   (a) a degree of advertising sufficient to ensure opening-up to competition; and

   (b) impartiality within the procurement procedure.[16]

   Therefore POL will need to run a fair and open competition. This would include setting out clear rules and criteria for assessment of responses which are then subsequently applied and ensuring that bidders are afforded a proportionate time to respond to any opportunity.[17]

   Below threshold procurements which attract cross border interest cannot lawfully be made by way of direct awards or by way of closed competitions (i.e. with a pre identified pool of bidders).

12

[14] However, in the event of a challenge, it is for the challenger to show that cross border interest is present, rather than to simply demonstrate that its presence cannot be discounted *Tecnoedi Costruzioni*,C-318/15

[15] See for example *Strong Segurança*,C-95/10

[16] *Coditel Brabant*,C-324/07

[17] CCS Guidance recommends that where the contracting authority is seeking a tender response, bidders should be afforded at least 10 working days to respond *Guidance on the new transparency requirements for publishing on Contracts Finder*

POL00401629

FN7 - Interplay with the Regulations

The Regulations impose certain obligations in respect of below threshold contracts ≥£25k. These obligations do not apply where, had the procurement been at or above OJEU threshold, it would have benefitted from an exemption from the Regulations.[18]

1. **Requirements to publish contract opportunities on Contracts Finder**

   POL must publish contract opportunities on Contracts Finder in relation to opportunities ≥£25k whenever it advertises the contract opportunity elsewhere (for example on the POL website or in trade press). "Advertisement" for these purposes is broadly interpreted but will not apply where POL simply obtains quotes from one or two selected contractors.[19]

   The information must be published on Contracts Finder within 24 hrs of publication elsewhere.

   Contracts Finder information must include:

   (a) The date and time by which any interested supplier must respond if it wishes to be considered (which must be a sufficient but not disproportionate period of time within which to respond).

   (b) How and to whom a supplier must respond.

   (c) Any other requirements for participating in the procurement.

   POL must also offer unrestricted and full direct internet access free of charge to any relevant contract documents[20] (unless a relevant reason for not doing so applies)[21].

2. **Requirement to publish contract award details**

   POL is required to publish contract award details in Contracts Finder for contracts ≥ £25k within a reasonable time of awarding the contract.[22]

   Contracts Finder information must include:[23]

   (a) the name of the contractor;

   (b) the date on which the contract was entered into;

   (c) the value of the contract;

   (d) whether the contractor is a SME[24]; and

[18] Regulation 109(2). See exemptions contained in Regulations 7-17. Importantly, exemption does not appear to include Regulation 32 situations.

[19] CCS, *Guidance on the new transparency requirements for publishing on Contracts Finder*

[20] Regulation 110(15)

[21] Regulation 110(13) and for reasons see Regulation 53(3) and (4)

[22] CCS guidance recommends publication within 90 days of contract award

[23] Regulation 112

[24] For these purposes, "SME" means an enterprise falling within the category of micro, small and medium-sized enterprises defined by the Commission Recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises.

DRAFT

POL00401629

(e) whether the contractor is a VCSE[25].

POL can withhold information where one of the grounds in Regulation 112(2) applies.

3. **Prohibition on separate prequalification stage**

POL is prohibited from using a separate prequalification stage for contracts of £25,000 to £189,329.[26] POL may ask relevant and proportionate "suitability assessment" questions as part of a one stage process.[27]

Potential consequences of a failure to conduct a process:

Scenario 1: No cross border interest, no POL procurement policy, <£25k contract therefore no Regulations

No procurement law consequences – POL has freedom to award as it considers appropriate including to make a direct award.

Scenario 2: No cross border interest and no POL procurement policy, ≥£25k contract therefore Regulations apply

Regulations require publication of opportunity and award on Contracts Finder and prohibit use of separate prequalification stage.

Failure to comply with Regulations - potential judicial review challenge e.g. on the basis of a breach of a statutory duty (subject to the challenger having sufficient "standing").

Scenario 3: No cross border interest, but the award is contrary to POL procurement policy (if applicable)

Potential judicial review challenge e.g. based on a breach of a legitimate expectation (subject to the challenger having sufficient standing).

(Compliance with the Regulations is required for contracts ≥£25k - for a failure to comply see scenario 2.)

Scenario 4: Where there is cross border interest.

A breach of the general treaty principles of non-discrimination, equal treatment, transparency and proportionality may currently be brought by way of a damages action on a basis of a breach of a statutory duty or could potentially be pursued by way of judicial review, subject to the necessary standing.

(Compliance with the Regulations is required for contracts ≥£25k - for a failure to comply see scenario 2.)

(Compliance with internal policy is also required – for a failure to comply see scenario 3.)

DRAFT

12

[25] For these purposes, "VCSE" means a non-governmental organisation that is value-driven and which principally reinvests its surpluses to further social, environmental or cultural objectives.

[26] This is based on the current threshold for supplies/services contracts for sub-central contracting authorities

[27] See Regulation 111(6) for definition of "suitability assessment question"

POL00401629

Consequences of Brexit

Under the European Union (Withdrawal) Act 2018, at the end of the Transition Period on 31 December 2020, breaches of the general treaty principles will no longer give rise to such a claim.

There is a transitional provision (which has not yet been commenced) within the 2018 Act to the effect that any actions for a breach that took place prior to the 31 December 2020 may still be brought until 31 December 2023. As such, if a cause of action for a breach of a general treaty principle arises during the Transition Period, it is likely that there will remain a period within which a challenger could raise an action.

DRAFT

Company Details

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

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

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

POL00401629

Procurement Risk Exception Form - Guidance



1.1. *Identifying the need for an exception*

If a business unit wants to extend a contract, or enter into a new contract, and Procurement advise that doing this will create a compliance breach of **any value over £25k**, then the contract owner or prospective contract-owner must complete the Procurement Risk Exception Form [PREN]. This, along with any supporting documentation requires Board level approval.

1.2. *Complete the Procurement Risk Exception Note*

The contract owner (or prospective contract owner) should complete all three sections of the PREN.

1.3. *Review & Approval of the Procurement Risk Exception Note*

On completion submit the form to Procurement for review, they will assure whether the form has sufficient detail included. The PREN should then be passed to the accountable GE Member (or delegate GE-1) for the area raising the risk and the Legal team for review and preparation of a Legal Risk Note.

On completion of all reviews, Procurement will submit the PREN alongside any additional information to GE and then the Board for approval.

Where delegated authority requires additional approvals, an accountable owner must be identified for on-going monitoring & closure of the exception. This must be noted on the PREN form.

1.4. *Recording & Monitoring of PREN*

The approved PREN must be recorded on the Procurement PCR Risk Register (PCRRR) and where material [>£189k over term of agreement], the local Business Risk Register in the form of an Open Risk to ensure the business area and the Risk Business Partner has full visibility of the exposure faced.

Based on the level of risk exposure the frequency of review will be assigned by Enterprise Risk. At the frequency defined, the Business Owner of the PREN should schedule review sessions with the accountable owner (GE Member), Procurement, Risk Business Partner and action owners of the PREN. This ensure progress is reviewed and any material changes which may affect the duration or actions in flight are given appropriate oversight and approval. Based on this review the local risk register and central exception tracker will be updated. Five working days prior to the Risk Exception End Date, a final review session should be held. This review will determine whether the PREN can be closed or whether an extension is required. If extending the PREN it will require re-approval by all original approvers including Board. A report of all outstanding exceptions is provided to the Risk & Compliance Committee at a 2 monthly frequency. Accountable GE/RCC members may be required to provide an update.

1.5. *PREN & REN Closure*

When the risk has been remediated either by corrective action or expiry of a statutory period, the exception can be closed. The closure rationale & supporting evidence including any updated documents (e.g. contracts etc.) must be agreed with the accountable owner and provided to the relevant Business Risk Partner within the Enterprise risk team (with evidence of owner agreement supplied). On receipt they will review all evidence, raise any queries as necessary and once satisfied close the risk. On closure they will notify all relevant parties.

POL00401629

Purchasing Process

[Draft for Approval]

Version – V0.1

12

POL00401629

1. Overview 3
1.1. Introduction by the Process Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 6
1.5. The Risk 6
1.6. Legislation 6
1.7. Purchasing Channels Guidance 6
2. Risk Appetite and Minimum Control Standards 11
2.1. Risk Appetite 11
2.2. Policy Framework 11
2.3. Who must comply? 11
2.4. Roles & Responsibilities 12
2.5. Minimum Control Standards 15
3. Definitions 17
3.1. Tools 17
3.2. Definitions 17
4. Where to go for help 18
4.1. Company Policies 18
4.2. How to raise a concern 18
4.3. Who to contact for more information 18
5. Governance 19
5.1. Governance Responsibilities 19
Governance 19
6. Control 20
6.1. Process Version 20
6.2. Process Approval 20
Company Details 20

12

[1]In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.

[2]In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

POL00401629

1. Overview

1.1. Introduction by the Process Owner

This Purchasing Process sets out the processes through which, the organisation acquires the goods and services it needs, using contracted suppliers and agreements, with defined and controlled purchasing channels from request through to payment.

1.2. Purpose

The purpose of this process is to ensure that the purchasing process for goods and services required for Post Office daily operations is done in a compliant, timely and efficient manner once an approved contract has been entered into with a third party, and the supplier successfully onboarded onto the Post Office purchasing system. The process provides guidelines and principles that Post Office employees will follow in the end to end purchasing process. At the same time it is an essential framework for the current and future business relationship with our suppliers.

It is one of a set of processes and policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Post Office. Compliance with these policies supports the Post Office in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

This Process will provide:

- Guidance on how goods and services must be purchased by Post Office employees.
- Overview of the purchasing channels, processes, when to use them, and what are acceptable and unacceptable purchases
- Corporate card maintenance and security
- Clarity on the roles and responsibilities for purchasing
- Misuse and abuse of corporate purchase cards
- Clarity in our approach to compliance by linking the Post Office Purchasing Process into the Procurement Policy

This process does not cover corporate policy on Travel and Subsistence, Procurement, Supplier Onboarding or Contract Management.

1.3. Core Principles

Purchasing shall be driven by the following Guiding Principles in all Purchasing activities:

Purchasing Principles

- Achieve sustained value by progressively managing Post Office expenditure, maximising value and seeking continuous improvement and innovation for the Post Office.
- Ensure the risk to Post Office is minimised by having contracts and commercial arrangements in place to ensure delivery of goods and services to agreed requirements
- Enable continuous improvement and compliance from our the relationships with suppliers.
- To ensure that only goods and services that are receipted are paid for and that waste and unnecessary expenditure is reduced; and to
- Ensure suppliers are paid within 30 days on undisputed invoices in accordance with

POL00401629

regulations for public sector bodies.

Purchasing Channels

- For spend to be managed within Post Office, Purchasing channels have been provided which are routes by which the business can buy goods or services through compliant methods. Each of these channels is a defined process with financial and audit controls and role requirements.

Buying Channel	User	Description	Purchasing Tools	Threshold
Catalogue	Business Users	• Purchase Order of standardised products and services with preferred suppliers through pre-negotiated contracts, such as Stationery, IT and Identity Checks	• Web3 • Service Now	• Unlimited • Approved by Delegated Authority
Manual Purchase Order	Business Users	• Purchase Order of products and services with pre-vetted suppliers through pre-negotiated contracts. • This represents he majority of the Post Office expenditure.	• Web3	• Unlimited • Approved by Delegated Authority
Corporate Purchase Card	Card Holders	• Purchasing on an ad-hoc, one off or emergency basis, with retrospective approval for under threshold purchases	• Selenity • CFS	• Limited to card thresholds
Automated invoicing	Business Users	• Transactions are ordered via supplier hosted external systems and are approved during creation, such as Travel, Fleet, Temporary Labour and Swindon Stock. • PO and Receipt are created automatically when the invoice is uploaded to the Post Office purchasing tool.	• Supplier hosted systems • Galaxy • CFS	• Unlimited • Approved via the external ordering process • Processed automatically
One Time Vendor OTV	HR & Finance	• For processing invoices related to the Leaving the Business with Dignity (LBD) process. • Payment of exceptional items	• CFS	• Pre-Approved to fixed thresholds and approved by Delegated Authority

Purchase Order Core Principles

- Post Office operates a 3 Way Match policy to auto release payment:
  - Purchase Order [PO] + Goods Received Note + Invoice
- Correct sequence needs to be followed for Manual PR:
  - Requisition - Purchase Order - Goods - Received - Invoice Payment
- A Supplier must have been through the onboarding due diligence system process to be set up on the Purchasing tool for use. This includes separate authorisations from the Procurement and Master Data teams and an independent verification of bank details from Treasury.
- Only the OTV and Corporate card channels allow for the use of suppliers who have not been through due diligence.
- No PO, No Pay policy enlists suppliers in compliance with the Post Office Policy by requesting a PO before goods or services are ordered.

POL00401629

- Exceptions to No PO No Pay are made for utilities, rates and other taxes were the PO is raised retrospectively and are listed in section 1.7.2.1.
- For NPIR and OTV channels a 2 Way match process applies to release payment: Authorisation + Invoice
- The Sarbanes-Oxley segregation of duties principle applies to separate the Requisitioner, Approver and Payer, thus protecting Post Office against errors, malicious intent and fraud.
- Procurement Operations are accountable for all Catalogue content
- Procurement Category Manager approval is required to ensure that the correct supplier is used and a Contract and CAF is in place for each purchase order to ensure PCR compliance.
- Financial approval is required to ensure that budget is available to make an expenditure commitment.

Corporate Card Spend Core Principles

- Cards must be used for Business purposes **only**.
- Goods and Services should be delivered to a Post Office business office address.
- The card is non-transferable.
- The card and PIN must be kept safe at all times.
- The card shall **not** be used for cash withdrawals.
- Employees must be authorised by their Finance Business Partner and Budget Holder before becoming a card holder.
- Transaction and monthly credit limits shall be established for each card issued.
- Budget holders may change the card limit by applying for an increase or decrease via the CPC Coordinator.
- The Card may not be used for travel related expenses (except for exceptions listed in 1.7.3.5) where Post Office mandates the use of the Travel Management Company for hotels, flights, rail travel and events booking. This is set out in further detail in 1.7.3.6.
- Use of the Card for any purpose which is not in accordance with company policy **will** result in disciplinary action.

Accounts Payable Principles

- Invoice should be sent directly by the supplier to Accounts Payable and not via an internal colleague - internal colleagues can be cc'd in if required
- Invoices must be sent containing a relevant Purchase Order number and relevant line number - as stated on the Purchase order
- Invoices should be submitted in a PDF format and in a consistent layout to enable data capture to be performed
- LBD [leaving the business with dignity] and compensation invoice payments must be fully approved, containing GL and cost centre prior to submission to Accounts Payable
- Invoices can be blocked for payment if in dispute
- Invoices in dispute must be reported to Accounts Payable and the Contract Manager, giving reason for dispute, supplier contact name and estimated date for resolution.
- Only fully authorised invoices will be paid, and will be paid in line with agreed payment terms - any terms other than 30 days need Finance Director
- Suppliers will be paid within 30 days of receipt of undisputed invoice,
- Suppliers will be paid by Bacs transfer. Any exception to this requires justification by means of business benefit.

POL00401629

- Any exceptional requests for payment via CHAPS will require a business benefit along with a 24 hours' notice to meet treasury timescales
- Payment runs are completed daily Monday to Friday, with exception of UK bank holidays

1.4. Application

This Process is applicable to all areas within the Post Office and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Post Office's Risk Appetite which is periodically reviewed by the Board.

In exceptional circumstances, where the purchasing activity sits outside of the Post Office's accepted Risk Appetite, a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team – https://poluk.sharepoint.com/sites/Risks

For definitions please see section 3.1.

1.5. The Risk

The Purchasing Process is designed to establish best practice and mitigate the risk . All purchasing activities shall adhere to the Post Office Purchasing Process. Procurement shall ensure that risk management is appropriately applied at all stages of procurement activities. Guidance shall be made available to enable the Procurement team to employ Post Offices risk management principles.

Purchasing activities following best practise shall be carried out in a manner that will enhance Post Offices capability to avoid waste and inefficiency, prevent fraud and unauthorised expensiture, and facilitiate the processing of supplier invoices in accordance with our payment terms.

1.6. Legislation

The Post Office seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- Supply of Goods and Services Act 1982
- The Reporting on Payment Practices and Performance Regulations 2017
- Public Contract Regulation 2015
- Competition Act 1998
- Concession Contracts Regulation 2016
- Companies (Audit, Investigations and Community Enterprise) Act of 2004
- Data Protection Act 2018
- Modern Slavery Act 2015

1.7. Purchasing Channels Guidance

1.7.1 Catalogue Summary

A Catalogue is pre-agreed list of prices for goods or services with our preferred suppliers. The use of a catalogue to create a requisition is therefore automatically compliant under contract. Where the catalogue is hosted on the supplier website (Punch-Out), an additional check is used by Procurement to ensure that the products selected are part of the agreed list and the pricing is accurate. In all other respects the process is the same as 1.7.2.

POL00401629

1.7.2 Manual Purchase Order Summary

A manual order is created by first raising a Purchase Requisition containing all the information required for the order including the name of the supplier and the accounting codes for the budget, nominal codes and tax. Pre-configured Web3 forms are available to guide the addition of essential information. Notes and attachments can be added.

The Requisition is sent for approval through the following routes:

- Buyer approval: the requisition will be routed to a buyer in Procurement if it is an incomplete non-category item, or the Requisitioner has included a buyer note.
- Budget approval: Web3 will then automatically check if there is enough budget against a code to proceed.
- User spend approval: Web3 will then check if there is any additional approval steps required specifically created for the user that has raised it.
- Product category approval: to verify if the chosen supplier is correct and a valid Contract is in place.
- Project spend/BAU spend approval: the relevant financial approver in projects or BAU teams (POL and POI) depending on the budget or cost centre concerned.

Once a Purchase Requisition is approved, it is automatically converted to a Purchase order. This creates a financial commitment in the CFS system and the order is sent to the supplier.

A Goods Receipt must be created once the goods or services have been delivered, to confirm acceptance and create an accrual in the CFS system.

The Web3 purchasing process works on the principle of a 3 way match of Purchase Order, Receipt and Invoice. The only exceptions to this would be those listed in 1.7.2.1, and in 1.7.4 and 1.7.5.

1.7.2.1 Exception to No PO No Pay

We have a "No purchase order, no payment" Policy with suppliers to ensure that we have an efficient and controlled payment process. A supplier should be provided with a valid purchase order (PO) number which must be quoted on all supplier invoices.

Suppliers are told to consider any request for goods or services without a PO as invalid as it may have been requested without company authorisation. Suppliers are also informed that any invoice that is submitted without a valid PO number will be returned, or held pending investigation and coding, which could delay processing and payment.

The only permissible exceptions to this rule are:

- Charitable donations
- General leases, which are subject to Direct Debits or standing orders (e.g. vehicle, and machinery)
- LBD Payments on behalf of individuals, made under the Leaving the Business with Dignity programme (e.g. legal fees and training grants)
- Non-procurement related payments to (or on behalf of) Public Bodies, made under legislative (or similar) obligations
- Utilities - electricity, gas, water, rates etc.
- Compensation payments

1.7.2.2 Approval and Delegation

Financial approval rules, levels and thresholds are set by the Financial Leadership Team and have been designed in such a way to prevent self-approval.

POL00401629

Only users allocated the licenced role of an approver can approve, in addition they must also be added to an approval table or be nominated as a delegate to actually approve a requisition.

Approvers can delegate their approval by using an out of office functionality to set delegation over a defined period, however they may only delegate to another Web3 user who has been given a system role as an approval.

Web3 also has the functionality to add an additional approver to the workflow if there are specific requirements against an individual, i.e. if the Requisitioner is a non-Post Office employee/ contractor.

1.7.3 Corporate Card Process Summary

The card process does not require competitive quotations but there is an expectation that the cardholder will seek the best price and value for the Post Office. Since all purchases must be under the relevant monthly limit set for the card, where the requirements change to regular use the requirement shall be referred to Procurement to review alternative supply options. For the avoidance of doubt regular use would be a recurring annual cost of more than £5,000 either as a one off payment or a series of small recurring payments from one or more card holder.

1.7.3.1 Card Maintenance

Name changes, card replacements, cancellations or reinstatements, are maintained by the CPC Coordinator with approvals and verification from the relevant Financial Director. Cost centre and department changes are made in coordination with Accounts Payable to enable the automated invoicing of card statements.

1.7.3.2 Card Security

Cards, PINs and accounts shall be issued to individual employees on the basis that they take adequate responsibility for the security of the cards, never display or give their card number or PIN to anyone for the purpose of allowing anyone else to place an order with the card. Sharing card details represents a fraudulent breach of contract with our card provider and a breach of GDPR. The Post Office does not tolerate fraud under any circumstances. The cardholder may be subject to investigation under the formal HR disciplinary procedure.

If a card is lost or stolen the cardholder is responsible for informing the card provider immediately and updating the CPC Coordinator at the first available opportunity.

1.7.3.3 Card Spending Limits

The cardholder transaction limit for monthly expenditure is set at £1000 on issue. Any increase to these limits shall be considered separately from the card holder application, except where this is a temporarily increased limit for an ad-hoc purchase. Transaction limits over £1000 must be approved by the Procurement Director and the accountable GE Member.

All transactions made on the card are retrospectively entered into the Selenity expenses system to enable the cardholder to attach receipts or other supporting evidence. Transactions are reviewed and approved retrospectively within Selenity by the cardholder's line manager.

1.7.3.4 Card Control

POL00401629

Cards will be assigned to one cost centre **only** and all purchases will be against that cost centre. The number of cards per cost centre will be at the discretion of the Finance Director. Cards shall not be used for the purposes of withdrawing cash and purchases shall not be split resulting in a number of transactions below the threshold; such transactions will be identifiable via the monthly MI reports.

The exception to this will be a card held centrally by Procurement to facilitate ad hoc purchases for departments without a CPC card, or for occasional purchases where payment can only be made via a credit card. An example of this is Software where company policy ordinarily precludes purchasing software outside of the CFS system. The CPC Procurement cardholder must hold email authorisation from both the Procurement Director, the Budget Holder and the IT Software Vendor Manager for the purchase and ensure that the costs are cross-charged appropriately.

1.7.3.5 Card Acceptable Purchases

Acceptable purchases are linked to the specific business role of the cardholder and are those purchases that cannot be managed by any other method, these could include:

- Emergency Vehicle Spares
- Emergency Burglary and Damage purchases
- Emergency Hostages Costs
- Toll Charges
- Ferry costs for Supply Chain
- SIA costs e.g. licences
- Hire fees (e.g. costumes etc. for Public Relations purposes)
- Ad hoc Courier services
- External Hospitality / Entertainment (In line with the gifts and hospitality process published on the Post Office Intranet)
- Conference/Meeting less than <£500

Also acceptable are non IT related subscriptions, non-operational licences (such as TV licenses for our buildings) and corporate memberships (like CIPS, CIPD etc.), as opposed to individual memberships (one per person) that should be reclaimed via the expenses system.

1.7.3.6 Card Unacceptable Purchases

Corporate Purchasing Cards **must** not be used for Goods and Services where a Post Office Contract exists, for Travel & Subsistence i.e. Train Tickets, Flights, Meals, Snacks, Petrol or Overnight Accommodation, and any of the following:

- Items exceeding the limit agreed by Budget Holder,
- Capital equipment
- T&S, personal travel, entertainment and group meals
- Reward and Recognition
- Personal items
- Consulting fees
- Lease contracts or long-term rental contracts.
- Externally arranged seminars
- Training (except with express permission in writing from the L&D team)
- Advertisements in newspapers and magazines
- Journals, business periodicals and magazines

POL00401629

- General stationery (ad hoc or otherwise)
- Photographers
- Ad hoc printing, laminating, binding etc.
- All conferences/meetings greater than > £500 are to be sourced via Post Office business venue finder, via the Post Office Travel Portal.
- Renewing subscriptions
- Software, unless with explicit authorisation from the IT Software Vendor Manager and the Procurement Director, and then only via the CPC Procurement Cardholder

1.7.3.7 Misuse or Abuse of Cards

Where Cards have been used for purposes which are not in accordance with company policy, the cardholder will be subject to investigation under the formal disciplinary procedure.

Post Office may investigate any fraudulent use of the Purchasing Card and where investigations uphold fraudulent use; Post Office will treat this as a serious disciplinary offence, and proceed under the conduct code. Where fraudulent use of the card by the cardholder, or someone the cardholder has knowingly allowed to fraudulently use the card is detected, the card will be cancelled immediately and necessary measures will be taken. Fraudulent use will be treated as gross misconduct and may result in summary dismissal.

Where a cardholder is found responsible for, or is party to the fraudulent use of the CPC, they will be required to repay the Business for any expenditure incurred. Post Office shall be entitled to recover the principle sum by way of a single deduction or a series of deductions from the cardholder's pay, including pay in lieu of notice or any other payment due on the termination of the employment.

Post Office may withdraw the cardholder's permission to use a card, at any time, whereby the card must be destroyed immediately.

1.7.4 Automated Invoicing Summary

The Automated invoicing process enables the bulk loading of consolidated invoicing from suppliers where either the purchasing activity and authorisation for expenditure takes place on a separate supplier hosted system (such as Travel, Fleet Repairs and Temporary Labour) or as part of another mechanism (Corporate purchase Card) and where the quantity and frequency of transactions is not suitable for a 3 way match.

The list of suppliers eligible for NPIR is restricted and any changes must be approved with Accounts Payable. Supplier list currently comprises of Intelligent Resource, Manpower, Brook Street, Capita, Caulders, Kinto (Inchape), Barclays, Leaseplan, and Rivus.

NPIR involves loading of a pre-approved multi line invoice into the CFS system which then automatically creates a matching PO to enable payment.

1.7.5 OTV Summary

One Time Vendor is used for exceptional payments as per 1.7.2.1 and is an exception to No PO NO PAY. All Leaving the Business with Dignity related invoices must be received following relevant checks in HR, and are coded to the correct GL and budget code. This process is subject to manual financial controls with the Accounts Payable team.

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Post Office will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Post Office is willing and able to tolerate.

The Post Office takes its legal and regulatory responsibilities seriously and consequently has:

- Tolerant risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- Averse risk appetite for litigation in relation to high profile cases/issues
- Averse risk appetite for ligation in relation to Financial Services matters
- Averse risk appetite for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the Group
- Averse Risk Appetite in relation to unethical behaviour by our staff.

The Post Office acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established a Procurement Policy and set of supporting processes which are subject to annual review. These are designed to ensure compliance with best practise while achieving value for money,combating waste and inefficiency, and complying with regulations.

The Purchasing Process is a key process under the Procurement Policy framework and should be considered and read in conjunction with the overarching Finance Policies, Delegation of Authority Policy and the Code of Conduct where relevant.

2.3. Who must comply?

This process applies to all employees who purchase from suppliers, this includes the approval of transactions and the processing of payments to suppliers. Compliance with this process is mandatory for all business units within POL and POMS.

In the case of agencies and consultancies, all contracted personnel working on behalf of POL shall be made aware of this process and shall comply with all procurement procedures listed within the Procurement department guidance.

All employees who procure from suppliers should work to our values Care, Challenge and Commit and our standards set out in the Code of Business Standards and the other POL policies listed in 4.1. All staff working on behalf of POL should not enter into supplier

POL00401629

selection, discussions with 3rd party, commitment to spend, material contractual changes or any procurement exercise without the involvement of the procurement team.

This process does not apply directly to outsourced service providers or to suppliers; however, by making sure that suppliers comply with our Supplier Code of Conduct it does seek to ensure our outsourced service providers and suppliers must: support the governance of POL; mitigate the risks faced by POL; and support the quality of service we provide to our customers, our policies and other legal requirements (including finance, health and safety, human rights and labour standards, and employment laws);

Where non-compliance is identified the matter must be referred to the Director of Risk, Compliance Director and the Procurement and Finance Directors. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

2.4. Roles & Responsibilities

Procurement shall drive the procurement process, negotiate commercial arrangements, and support the means by which procured solutions are delivered.

2.2 Roles & Responsibilities

Procurement Director is responsible for:

- Administering this policy on behalf of the CEO
- Developing and rolling out the supporting strategies to drive continual performance improvement.

Procurement Performance Manager is responsible for:

- Product Ownership of Web3 including the governance of the configuration, upgrade and release schedules, introduction of new functionality
- Monitoring the workflow and mechanisms within web3 that enable control and separation.
- Web3 Licence governance and contract management.
- Cooordination of S2S Operational Board for the ongoing adoption and improvement of Web3 in line with business requirements.
- Assessment of suppliers' purchasing practices (including ethical, sustainable measures), taking appropriate commercial action as necessary.

Procurement Operations and Purchase Order Team are responsible for:

- Driving, adopting and sharing best practice purchasing standards and initiatives to facilitate business adoption and prompt payment of suppliers;
- Supporting business to use the appropriate Purchasing Channels, including active support for Web3 user community
- Developing mutually beneficial collaborative trading relationships with suppliers;
- Monitoring the workflow and mechanisms within web3 that enable control and separation.

Directorate/Business Managing Directors are responsible for:

- Ensuring that this policy, supporting procedures and corrective actions are implemented and complied with; and
- Leading by example in protecting the POL brand and championing knowledge sharing across the divisions.

Managers are responsible for:

- Implementing and enforcing the processes and procedures;
- Ensuring that their people are aware of their responsibilities and receive appropriate training.

POL00401629

Suppliers are responsible for:

- Acting in accordance with this policy and associated procedures and guidance provided in their contracts and the Supplier Code of Conduct.

Roles specific to Purchasing Web3

- Accounts Payable are accountable for the timely processing of valid supplier invoices and credits and the release of payment. They are accountable for ensuring that all payments are in adherence to broader Finance and Treasury rules.
- Financial Approver and Project Manager are responsible for value based approval workflows for the approval of Purchase Requisitions and for changes to financial related information on Supplier records. They are determined by the delegation of authority thresholds and levels set by the Financial Leadership Team and are accountable for ensuring that appropriate checks are undertaken before approval is given.
- Functional Approvers are accountable for the non-value based approval workflows for the approval of Purchase Requisitions such as Category Management and for changes to non-financial related information on Supplier records. They are determined by the workflow requirements and are accountable for ensuring that appropriate checks are undertaken before approval is given.
- Procurement are accountable for the compliance based approval workflows for the approval of Purchase Requisitions and subsequent amendments to Purchase Orders. They are responsible for system content configuration management such as Catalogues, Forms and Category coding.
- Receipter is responsible the receipting is carried out in a timely manner and only once goods or services have been received in the business. They are responsible for ensuring that by creating a financial accrual, the Post Office is not paying for items that have not been received.
- Requisitioner is accountable for the compliant raising of requisitions with adequate information and detail to enable approver to approve and for suppliers to deliver. They are responsible for ensuring that the correct coding and detail is included and that they have appropriate authority to make a financial commitment.
- System Administrators are responsible for the maintenance of business model system data such as cost centres, approval tables, suppliers and user roles. They are determined by their roles within Master Data and are accountable for ensuring that appropriate checks and processes are followed.

Roles Specific to Purchasing via Corporate Card

- Budget Holders and Line Managers are accountable and liable for the compliance of all spend charged to the CPC, and for ensuring the appropriate use of the CPC. They are also responsible for checking the statements and the supporting information on a monthly basis via the expenses system. Access to the expenses system will be given to cardholders and their Line Managers. Budget Holders and Line Managers **must** evidence that control checks have taken place as and when requested.
- Cardholders are responsible for complying with section 1.7.3 of this policy. In the instance an audit is conducted they **must** be able to produce evidence of receipts and invoices, or proof that the transaction has occurred and goods have been received. Where an error is discovered, cardholders are responsible for addressing the error as outlined in 1.7.3.7. Incident notification and escalations should be made to the CPC Coordinator.

POL00401629

- Line Managers are responsible for updating the CPC Coordinator when a cardholder leaves the Post Office, and for ensuring that cards have been returned and destroyed when a cardholder leaves or, complying with section 1.7.3.7, when a cardholder's permission has been withdrawn. The CPC Coordinator shall also receive notification from HR of any involuntary leavers as part of the HR Leavers Checklist.
- The CPC Coordinator is the point of contact at Post Office. They are accountable for liaising with the card issuer for new card provision, card cancellations and portal management, internally managing the account and managing the relationship with the card provider in an operational capacity. They will also carry out an audit annually of cards and spend over the previous year.

  Where Cards have been used for purposes which are not in accordance with company policy, the CPC Coordinator must notify both the Procurement Director and the Finance Controls Team. The cardholder may be subject to investigation under the formal HR disciplinary procedure.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

POL00401629

2.5. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
CPC	Cardholder leaving the business without CPC being deactivated	Procurement Operations receive automated leavers notifications which are check against the cardholder list.	Procurement Operations	Ongoing
CPC	CPC used for non-compliant expenditure	CPC cards are blocked for cash withdrawal. All transactions must be evidenced and are retrospectively approved by line managers. Outstanding transactions are monitored	Internal Audit/ Procurement Operations	Ongoing
Purchasing	Non- permanent POL staff raising unsuitable orders	Contractors can be subject to additional "user" approval as a condition for granting system access. Web3 does not allow self-approval.	Procurement Operations	Ongoing
Purchasing	POL pays for goods or services that have not been received	Web3 works on a 3 way match and therefore goods and services must be actively receipted to enable invoice payment. No PO No Pay rules require all invoices to reference a valid order.	Accounts Payable	Ongoing
Purchasing	POL consumption of goods and services rises above intended budgeted levels	All purchases must be approved before an order is sent to a supplier. No PO No Pay rules require all invoices to reference a valid order.	Accounts Payable	Ongoing
Purchasing	Delegation of authority to approve is given to unsuitable people or in incorrect circumstances	Approvers cannot delegate to anyone. They can only delegate to another person with an existing approval role in web3.	Procurement Operations	Ongoing

POL00401629

		Delegation can only be set in absence by Master Data if first authorised by a line manager. Reports to monitor delegation and prolonged use of delegation is available for audit purposes.		
Purchasing	Requisitions are raised that are non-compliant with PCR and/ or contracted limits	All purchase requisitions are reviewed by Procurement to ensure a Contract and CAF are in place and PCR thresholds are not exceeded	Procurement	Ongoing
Purchasing	Requisitions are raised without suitable approval, resulting inappropriate expenditure or fraud	Approval roles, levels and thresholds are agreed by the Finance Leadership team and controls on changes to approval tables are in place. All Requisitions in Web3 have an automated approval workflow determined by Cost Centre or Project Code. Web3 does not allow self-approval.	Procurement Operations	Ongoing
Purchasing	Insufficient checks on bank accounts, resulting in payments made to the wrong entity or fraud.	The creation and amendment of supplier bank details is independently verified by Treasury before being activated in Web3	Master Data	Ongoing
Purchasing	Separation of duty when creating and amending supplier payment details	The creation of a supplier record requires the approval of 3 teams Master Data, Procurement Operations and Treasury. Changes initiated by suppliers or requested by Procurement Operations can only be accepted when approved by all three team. Any changes to supplier records produces notification and is recorded in an audit trail.	Master Data	Ongoing
Purchasing	Payment processing and payment performance to agreed terms is delayed by a failure of users to receipt purchase orders	Reports are available to monitor timely receipting. The POL Purchase Order team and Procurement Operations support and encourage receipting in a timely manner	Procurement Operations	Ongoing

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

3. Definitions

3.1. Tools

1. **Web3** Source to Settle system - Sourcing and Contract Management through to Purchase to Pay modules
2. **CFS** Central Finance System – linked to Web3 via an interface for all transactions and also used directly for the processing of NPIR and OTV transactions
3. **Selenity** – Expenses system used for the retrospective approve of Corporate Purchase Card transactions
4. **Service Now** – IT Service Desk system used for the catalogue purchasing of IT kit and the RTQ (request a quote) service with IT suppliers.

3.2. Definitions

1. **CAF** – Contract Authorisation Form
2. **CIPD** – Chartered Institute of Personnel and Development
3. **CIPS** – Chartered Institute of Purchasing and Supply
4. **CPC** – Corporate Purchase Card
5. **GDPR** – General Data Protection Regulation
6. **MI** – Management Information
7. **OTV** – One Time Vendor
8. **PCR**– Public Contract Regulations 2015 are rules on the procedures for procurement by contracting authorities with respect to public contracts.
9. **PIN** – Personal Identity Number
10. **POI** - Post Office Insurance – the Post Office Insurance business which is separate from the POL in regard to public subsidy
11. **POL** – Post Office Limited entities and subsidiaries
12. **Sarbanes-Oxley** – the Sarbanes-Oxley Act 2002 is USA legislation but separation of duty and financial controls principles have been adopted as best practice for purchasing processes and associated purchasing tools and systems.
13. .**S2S** – Source to Settle
14. **SIA** – Security Industry Authority
15. **T&C** – Terms and Conditions
16. **T&S** – Travel and Subsistence

POL00401629

4. Where to go for help

4.1. Company Policies

The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to report without any undue delay.

Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: GRO or by telephone on: GRO.
- The confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO, or
- Via a secure on-line web portal: http://postoffice.ethicspoint.com/

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Correspondence Team.

Post Office encourages members of the public or people not employed by us who suspect [*activity in breach of process*] to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Procurement Director.

12

POL00401629

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the Procurement Director of Post Office Limited.

The Policy owner is the Procurement Director who is responsible for ensuring that the Procurement Department conducts an annual review of this Policy and tests compliance across the Group. Additionally, the Procurement Director and the Procurement Department are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

Governance

- To ensure effective governance of the Purchasing processes and purchasing tools by having the governance of a cross functional board of stakeholders (the S2S Operational Board) who hold the authority for changes to the process, controls and underlying data. This board reports to a S2S Steering Committee for key decisions.
- This policy must be reviewed and approved by the Procurement Director and the Accounts Payable Manager on an annual basis, except where a significant change in policy requires the review and approval of Post Office Group Executive (GE). All consequent revisions must be fully documented in the modification history section of this document.
- Relevant procedures must be updated to conform to the policy and updated following approval by the Post Office Group Executive. Changes to the policy must be communicated to the S2S Operational Board, noted in Section 3 Definitions of this policy document. Those staff listed must, in turn, ensure that the changes are cascaded to staff and/or 3rd parties as appropriate.

POL00401629

6. Control

6.1. Process Version

Date	Version	Updated by	Change Details
13/08/2020	0.1	Susan Godfrey	Draft Version
	0.2		

6.2. Process Approval

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

Committee	Date Approved
POL R&CC	
POMS R&CC	
POL ARC	
POMS ARC	

Process Sponsor: [*name of policy sponsor*]

Process Owner: Procurement Director

Process Author: Procurement Performance & Operations Manager

Next review: [*date of next review in DD MM YYYY format*]

Company Details

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

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

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

POL00401629

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Policy Update	**Meeting Date:**	10th September 2020
Author:	Reena Chohan	**Sponsor:**	Jonathan Hill/Ben Foat

Input Sought:

Discussion:

The Committee is asked to review and approve the updated Policies and endorse the proposed actions for the business to take these forward.

Executive Summary

This paper provides a summary of changes that have been made to the policies below as part of their annual review process for the RCC to consider.

Questions addressed in this paper?

1. Which policies were updated in this annual cycle review?
2. What updates were included and why?

Which policies were updated in this annual cycle review?

1. In this review cycle the following **4** policies were revised, reviewed and updated as per the annual review process.

Policy	Last Reviewed	Updates	GE Owner	Governance Approval Body
Contract Execution Policy	September 2019	Minor updates to paragraphs within the Policy	Ben Foat	RCC & ARC
Vulnerable Customer Policy	September 2019	Minor update and updates made to legislative references	Ben Foat	RCC & ARC
Physical Security Policy	September 2019	Minor updates, how to raise a concern section amended with new Whistleblowing details.	Alisdair Cameron	RCC & ARC
HMRC Fit and Proper Standards Policy	September 2019	Minor updates following business structure changes	Ben Foat	RCC & ARC

12

What updates were included and why?

[Confidentiality Classification]

POL00401629

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

Contract Execution Policy: Amendments made to the following Paragraphs -

- Para 1.5:

Amended to streamline and clarify acceptable methods of execution in table format which is more user friendly.

Amended to include process for urgent execution using scanned signatures if permitted by the Company Secretariat to enable swift execution when required and must be permitted by the Company Secretary (control advised by Risk). This situation has arisen when executing contracts and the change makes it easier for the Company Secretariat and the business to ensure commercial transactions can be done quickly. Legal (Nick Baldock) have confirmed that this process is acceptable as set out in the policy.

- Para 1.5.3:

Amended to permit execution of deeds via electronic signature. During COVID-19, it was difficult and cumbersome to execute under seal or by wet signature and a risk exception had to be agreed. Update guidance from the Law Society confirms deeds may be signed electronically and this has therefore been reflected in the policy. Legal (Nick Baldock) have reviewed this change and approved.

- Para 1.6 & 1.7:

Amended to be clearer on the Exceptions and Breaches process for all Group Companies. The previous policy did not address the subsidiary risk exception process. This has been rectified. Having had the policy in operation for a year, it became apparent that operationally the process for recording breaches was not optimal (when discussed with Risk (Sukh Giller)). This has therefore been updated to ensure it is clear to ensure adherence.

- Para 2.2:

Amended the Policy Framework to reflect the current policies applicable to the Group, following consultation with Reena Chohan (People and Policy Compliance Manager) and other relevant policies which had not previously been mentioned (Procurement Policy, Contract Management Framework and the Risk Management Framework).

- Para 2.4:

Minor amendments to the language used to ensure that it is truly applicable to the Group* and its new Governance Framework (for example, eCAF is only applicable to Post Office Limited, not its subsidiaries and the new Governance Framework uses the term "spend approval limits" instead of "delegated authorities"). Other amendments reflect the change in the team structure (Retail – Retail & Franchise Network) and Franchise agreements should instead be Network agreements as per para 6.2.1.

- Para 5.1:

Minor amendments to job titles and language to reflect changes in organisational structure and revised language of the Governance Framework.

[Confidentiality Classification]

POL00401629

- Para 7.2:

Amendment to show the ARC as the oversight committee for the policy. It was not initially intended that this policy be approved by the ARC as it is an operational policy, however it was included in the Key Policy List and therefore approval is now required (the ARC approved the policy in September 2019). The ARC Chair has confirmed this policy should be approved by the ARC on this occasion.

- Para 5/6:

Moving of section 6 (Appendix referring to the Contract Approval Process) into section 5 (Governance) at the request of the ARC Chair.

- *This policy is intended to be adopted by all Group Companies, including Payzone Bill Payments Limited. The policy has been discussed with their Risk team.

Policy Compliance View

The Annual Review of the Policy conducted by the Policy Owner suggests that the Policy demonstrates conformance for each Minimum Control Standard through the appropriate governance structure in place for the execution of contracts within the Group. There are clear procedures and guidance in place to ensure risk is mitigated and that the group does not enter contracts without proper scrutiny which could lead the Group to potential financial losses. The Policy Owner has demonstrated how the minimum control standards stated within the Policy are being met in pursuit of day to day business.

Vulnerable Customer Policy: The annual update includes minor tidying up and some updates to the legislative references. The external accessibility experts Kate Nash Associates/Purple Space have reviewed the latest policy and confirmed that it is up to date and appropriate.

Policy Compliance view

It is useful to have endorsement from third party experts on the policy content, we have also had overall positive inspections from Citizen's Advice Bureau teams on branch accessibility. However, we could face challenges on digital accessibility and from recent FCA and Ofcom rules that continually 'raise the bar' on expectations. So continued focus is required in this area

Physical Security Policy: The annual review update includes minor changes such as updates to the How to Raise a Concern Section and minor tidying up of the Policy.
The Physical Security Policy Suite is one of a set of sub-policies set out below, this being the overarching policy:

12

- CCTV Deployment Policy and Code of Practice
- Lone Worker Policy
- Tiger Kidnap or Hostage Policy
- Incident Management Policy
- Overseas Travel Policy

Policy Compliance View

The Annual Review of the Policy conducted by the Policy Owner suggests that the Minimum control standards are set out and managed, however was unable to provide further evidence on how these are being met consistently through

[Confidentiality Classification]

POL00401629

day to day business and weather the risks around Physical Security are in line with the appropriate governance structure of the Group.

Compliance will look to conduct a more in-depth assurance review and sample test the Physical Security Policy Suite on a risk basis to review the policy standard and policy compliance in Q3.

The Policy is one of a set of security policies for the Group and therefore the minimum control standards stated within the policy form a part of wider key policies. The assurance will test how the Physical Security Policy is performing against the other subset of policies it belongs to and how effective the minimum operating standards relating to the management of our physical security risks are in pursuit of managing our business.

HMRC Fit and Proper Standards Policy: Amended following business structure changes, role titles and changes to process/ownership following completion of agent F&P project:

- Agent definition updated to reflect currently approved definition in AML/CTF policy
- Amendments for direct employees to reflect that Success Factors now includes a mandatory field to show whether a role is subject to HMRC F&P
- Removed requirement for direct employees transferring to a F&P role to be re-vetted as all individuals are vetted on employment and undertake annual re-declaration as there is on-going performance management and Business Code of Conduct, plus HMRC undertake some checks as part of the F&P process
- Updated references to Declarations Oversight Committee as this only covers agent F&P
- Updated whistleblowing contact details
- All role titles amended to reflect current structure and added roles of Head of Risk & Branch Standards and SmartID Product Owner as this area is now responsible for the Agent F&P Team (agent F&P declarations and reporting)
- Complete re-write of training matrix with input from impacted teams

Policy Compliance View

The project to deliver the system and processes for agent F&P declarations, reporting and governance was delivered in July 2020, and the minimum control standards in the policy standard have operated sub-optimally up to this point. For direct employees, records had not always been up to date, but in the last 6 months work has been undertaken with the Head of HR Organisation Effectiveness and Success Factors to bring all records up to date and implement controls to prevent issues.
Given the gaps previously identified assurance will take form over the next 12 months to ensure the minimum control standards in the revised policy standard will be brought into scope for quarterly checking by the Financial Crime team and the People & Policy Compliance Manager.

12

Assurance

Compliance have now introduced an assurance process for future policy submissions and re-review by requiring policy owners to attest that the minimum control standards stated within the policy are being met and can be demonstrated. *(refer to appendix A)*. The Policy Approval Form asks Policy Owners to complete a section on Policy Performance where they have to confirm that each minimum control standard stated within the policy is being met and can be evidenced. Compliance will give an initial view on this attestation within the template.

As this process now moves towards BAU from Q3 we would propose to do a more in-depth sample test some of these policies on a risk basis to review the policy standard and policy compliance. *(refer to appendix B as an example of how the testing will be carried out).*

[Confidentiality Classification]

POL00401629

We are currently in the process of updating the Key Policies Intranet Page which we propose to go live in Q3. The page will reflect the following:

- A policy summary of each key policy;
- Policy cycle document to show when policies were last reviewed and are due for their next review;
- Policy Approval Form;
- All Group Key Policies.

Progress

Good progress has been made in working with Company Secretariat in re-establishing the key policy list for appropriate review and regular sign off as well as identifying any gaps, however, there needs to be increased focus on ensuring policies are reviewed in accordance with the policy review cycle as we still have some gaps where policies are still out of date and do not reflect current working practices. *(refer to appendix C which highlights red flags on the policies which have been out of scope for some time now).*

Conclusion

We continue to work with Policy Owners and Company Secretariat to ensure we maintain our policy governance responsibilities. This is a key part of the wider Post Office controls work that is covered in the main paper.

[Confidentiality Classification]

POL00401629

Policy Paper Appendix A

Policy Approval Form

Applies to all Policy Owners who are submitting their policies for approval and sign off from RCC/ARC

This form is to be used for the approval of policies that are new/superseding, undergoing their annual review process or need any major amendments*

1. Policy Title

Please enter the name of the Policy

2. Reason For Policy Change

Tick appropriate box(s).

Please click the following link to see if the Policy forms a part of the Group Key Policy List

https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1

New and/or superseding	☐	Key Policy	
Annual Review	☐	Yes	☐
Major Amendment*	☐	No	☐
Minor Amendment	☐		

*A major amendment means a change to the purpose or intent of the policy. For example, new or amended legislation/regulation, updated principles or substantial content changes.

3. Policy Owner/GE Sponsor and Policy Review Dates

Policy GE Sponsor		Last Review Date	
Policy Owner		Next review Date	

4. Purpose of the Changes/Updates to the Policy

Please provide a summary to outline the changes/updates and amendments being made to the policy and clearly state the sections that have been updated and the reason.

12

POL00401629

5. Policy Performance

Policy owner to confirm below that each minimum control standard stated within the policy is being met and can be evidenced. Detailed commentary is not required for each control a simple attestation will suffice. However, the policy owner should be able to provide for each minimum control standard, evidence if challenged by Compliance, RCC or ARC that the minimum control standard is working. See example in notes below

6. Related Sub Policies/Processes

Please outline if there are any sub policies/processes that are linked to this policy and provide them as an attachment. What is the approval process for these sub procedures?

This section below should be completed by RCC.

7. Policy Approval By RCC/ARC

RCC	
Date Policy Approved	
No Further Action Required	

This section should be completed by ARC.

ARC	
Policy Approved	

12

8. POMS Policy approval where relevant

POMS RCC date	
POMS ARC date	

POL00401629

9. **Compliance assessment of policy review performance and evidencing minimum standards**

Notes to completing the Policy Approval Form Pre-submission checklist

Policy Template	Ensure the correct Policy type template has been used
Content	Ensure the policy includes the following if applicable to the policy: Overview Introduction by the Policy Owner Purpose Core Principles Objectives Application The Risk Legislation/Regulation and Industry Guidance Risk Appetite and Minimum Control Standards Policy Framework Who must comply? Tools & Definitions Where to go for help Additional Policies How to raise a concern Who to contact for more information Governance Responsibilities Glossary of terms Control Version Policy Approval
Formatting and language	Has plain English and the POL corporate visual identity been used as far as possible in the development of this new or amended policy

POL00401629

Hyperlinks	Have all hyperlinks used throughout the Policy been checked to ensure they are correct and working?
Website	Most group policies should appear on the PO intranet once approved with a few exceptions, please liaise with the Policy Owner if you are unclear on this.

Minimum control standards and evidencing compliance

Below is an example of how a control standard can be operated as working.

Policy AML CTF

Risk area

Through inadequate training, staff allow money laundering or terrorist financing to take place, resulting in reputation damage and regulatory fines.

Preventative Control:

Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training tailored to business risk areas.

Comment on the control

This control can be evidenced as working. An annual AML training and test is conducted. We can evidence both through Success Factors and Smart ID controls in the Network that this training and test is undertaken. There are also a wide variety of communications on this area that can be evidenced to raise awareness. This does raise AML awareness as evidenced through widespread knowledge of grapevine and the SAR process/submissions we receive.

POL00401629

Policy Paper Appendix B

Compliance

Policy Monitoring Report

Customer Communications and Financial Promotions *(for example purposes only)*

July 2020

SAMPLE

12

Contents

1. Overview

POL00401629

2. Objective of the review

3. Methodology

4. Source of information/References

5. Findings

6. Recommendations

7. Rating / Residual Risk Score

8. Managers Response

9. Agreed actions to be taken

10. Appendix

SAMPLE

1. Overview

POL00401629

The purpose of the Policy Monitoring Report is to understand, test and gain assurance that the Policies and Procedures Post Office Limited have in place are working and are fit for purpose.

Each Policy has been established to set the minimum operating standards, which provides a clear risk and governance framework and an effective system of internal controls for the management of risks across the Group.

Compliance with all policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

The below table sets out the Residual Risk Score and Rating that will apply upon review of each key policy to determine how effective the policy is, any control weaknesses or gaps and whether the policy needs enhancements/improvements.

Ratings	Residual Risk Score	
1	Satisfactory – no findings	Insignificant
2	Satisfactory – with findings	Low
3	Satisfactory – room for improvement	Medium
4	Unsatisfactory – improvement control weakness	High
5	Unsatisfactory – major control weakness	Critical

DRAFT

2. Objective of the review

POL00401629

To establish whether the customer communications and financial promotions Policy and the processes held within the policy are being adhered to by all employees and the effectiveness of the policy is being implemented across the group.

The customer communications policy and financial promotions policy requires appropriate care to be taken when communicating with customers, complying with the FCA principles for Business, particularly Principle 7 which outlines communications with customers – "firms must pay due regard to the information needs of their customers, and communicate information to them in a way which is clear, fair and not misleading."

All communications must be:

- Balanced;
- Balanced between risks and benefits;
- Accurate;
- Consistent;
- Not make untrue or misleading claims;
- Use appropriate language;
- Not seek to exclude, or restrict any duty or liability the Group may have to the customer;
- Not disguise, omit, diminish or obscure important information, statements or warnings;

There are two subsets from the FCA Handbook that are applicable and subjected to the customer communications and financial promotions policy:

a. Customer Lending – which is subject to the FCA's conduct of Business Source Book "COBS" and the Consumer Credit Sourcebook "CONC" being applied to customer communications and financial promotions.

b. Customer Savings – which is subject to the FCA's Banking Conduct of Business Sourcebook "BCOBS"

An initial review of the customer communications and financial promotions policy will be conducted in July 2020 with a view to review annually, depending on the outcome of this review.

12

3. Methodology

The review consisted of the following:

POL00401629

- Review of the customer communications and financial promotions Policy
- A sample check of two pieces of customer communications
- A sample check of two pieces of financial promotions which have been signed off
- A sample check of two areas of the policy to see if they are working in practice and that the processes written within them are being followed and adhered to within the business and applied to everyday work ethics.

4. Source of Information/References

The source of the information will come from:

- Marketing of our products and services
- Website or communications gone out to customers
- Customer communications and financial promotions policy

5. Findings

The review compromised of monitoring two signed off customer communications, two signed of marketing campaigns and two areas of the customer communications and financial promotions policy. In particular paying focus to weather employees were following current guidelines set out in the policy when writing or communicating with customers, following regulation and legislation when creating marketing material around our products and services and two areas of the minimum control standards which are in place to ensure and manage the risks so they remain within the defined Risk Appetite statements.

Whilst the above were followed and compliant as per the policy guidelines and standards there were other gaps identified within the policy such as, no documented process on how financial promotions are currently being approved and logged. At present a financial promotion has to go through several stages between the compliance team and other areas of the business before it gets approved, the policy itself needs enhancements in terms of adding in a structure of the approval process, ownership and record keeping of all approvals and declines to demonstrate a clear audit trail and to ensure all approved customer communications and marketing campaigns are within the defined risk appetite and are in line with current FCA and advertising standard agency regulations.

The approval log that is currently in place is not being utilised fully and needs enhancing to demonstrate that the appropriate level of checks are being done before final sign off and approval.

6. Recommendations

Whist the policy is effective and fit for purpose, it is recommended that the policy is enhanced and improved to demonstrate a clear sign off and ownership process is defined within the policy and sets out a structure on keeping a record of all approved and declined

POL00401629

customer communications and financial promotions to ensure that there is a clear audit trail of how they are being approved by the business.

7. Rating / Residual Risk Score

- Rating – Satisfactory, room for improvement
- Residual Risk Score - Low

8. Managers Response

It is clear that there is no sufficient process defined within the policy for documenting sign off for customer communications and financial promotions as well as where the ownership of this lies. The policy also does not demonstrate a process flow or guidance notes on how to manage and keep records/logs of approved of declined communications and financial promotions for audit purposes and to ensure our risk appetite is being met in accordance with regulation and our defined minimum control standards.

The current log is not being fully utilised and needs improvements to demonstrate the appropriate level of checks are being carried out before final sign off and approval.

It is evident that improvements/enhancements need to be made to the policy to ensure Post Office can demonstrate that they are being compliant on customer communications and financial promotions in accordance with regulation and meeting the FCA objective of "clear, fair and not misleading"

We will review what tools are available to make the relevant changes and enhancements to the policy and report back by September 2020.

9. Agreed actions to be taken

Action	Owner	Date to be completed by

POL00401629

Define a clear approval and ownership process within the policy		
A checklist/guidance notes to be compiled within the policy for appropriate sign offs and approvals		
A log/register to be implemented to demonstrate a clear audit trail for all approvals and declines of customer communications and financial promotions to ensure they are within the defined risk appetite and meet the minimum control standards.		

SAMPLE

10. Appendix

Policy Review Date	Next Policy Review	Review Conducted	Review Signed Off

POL00401629

	Date	By	By

SAMPLE

POL00401629

Policy Paper Appendix C

Policy Paper Appendix C

DRAFT

POL00401629

Policy Paper Appendix C

1. Group Key Policy Framework

The table from the suite of our key policy framework. Details are provided of Policy Sponsors (GE Members), status of the policy review and the governance body for the ultimate approval.

DRAFT

RED - Policies which are currently out of date/being drafted/not in use

AMBER – Policies currently being submitted for sign off, following annual review

GREEN - Policy Annual Review Complete no further action required until next review date

Department	Key Policy Framework (Risk Universe)	Version Control	Policy Sponsor (GE Owner)	Policy Owner	Last Reviewed (Annually)	Next Review Date	Governance Approval Body	Current
	Corporate Services							
Corporate Governance	1. Conflicts of Interest	2.0	Ben Foat	Sarah Koniarski	May 2019		RCC & ARC	No
	2. Whistleblowing	5.0	Ben Foat	Whistleblowing Officer	July 2020	July 2021	RCC & ARC	Yes
	3. Contract Execution Policy	0.1	Ben Foat	Rebecca Whibley	Sept 2019	Moved to Nov RCC/ARC	RCC	Yes
	4. Modern Slavery Statement	2019/ 2020	Amanda jones	Andy Kingham	July 2019	Sept Board	RCC & ARC	Yes

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Policy Paper Appendix C

Risk	5. Risk Appetite Statement		Alisdair Cameron	Mark Baldock	May 2016	Currently being drafted	RCC & ARC	No
	6. Risk Policy	1.0	Alisdair Cameron	Mark Baldock	Nov 2019	Nov 2020	RCC & ARC	Yes
Financial Crime	7. Financial Crime Policy	5.0	Ben Foat	Sally Smith	July 2020	July 2021	RCC & ARC	Yes
	8. Anti-Money Laundering & CTF Policy	6.2	Ben Foat	Sally Smith	July 2020	July 2021	RCC & ARC	Yes
	9. Vulnerable Customer Policy	3.0	Ben Foat	Paul Beaumont	Sept 2019	Sept RCC/ARC	RCC & ARC	Yes
	10. Anti-Bribery & Corruption Policy (Including Gifts & Hospitality)	4.2	Ben Foat	Sally Smith	July 2020	July 2021	RCC & ARC	Yes
Business Continuity	11. Business Continuity Management Policy	2.6	CIO - Jeff Smyth	CISO - Tony Jowett and Tim Armit	July 2020	March 2021	RCC & ARC	Yes
	12. Change Management Policy	1.5	Dan Zinner	Strategic Portfolio Director	Nov 2019	Nov 2020	RCC & ARC	Yes
Legal	13. Investigations Policy	1.0	Ben Foat		Sept 2016	Currently being drafted	RCC & ARC	No
Data Protection	14. Freedom Of information Policy		Ben Foat	Chris Russell	TBC	TBC	RCC & ARC	n/a
	15. Protecting Personal Data Policy	2.0	Ben Foat	Chris Russell	Dec 2019	Oct 2020	RCC & ARC	Yes
	16. Law Enforcement Agencies Policy				Being reviewed		RCC & ARC	Yes
	17. Document Retention Policy	1.2	Jeff Smyth	Ehtsham Ali	July 2020	July 2021	RCC & ARC	Yes
Internal Audit	18. Internal Audit Charter Policy	2020	CFO Allister Cameron	Head of Internal Audit Johann Appel	May 2020	May 2021	RCC & ARC	Yes
	19. Cyber & Information Security Policy	1.5	Jeff Smyth	Tony Jowett	Jan 2020	Jan 2021	RCC & ARC	Yes

DRAFT

POL00401629

Policy Paper Appendix C

Procurement	20. Procurement Policy	1.0	Alisdair Cameron	Barbara Brannon	Mar 2014		RCC & ARC	Yes
Health & Safety	21. Health & Safety Policy	2019	Alisdair Cameron	Martin Hopcroft	Oct 2019	Nov 2020	RCC & ARC	Yes
Physical Security	22. Physical Security Policy/Suite	2.1	Julie Thomas	Tim Perkins	Sept 2019	Sept RCC/ARC	RCC & ARC	Yes
Human Resources								
	23. Conduct Code Procedure	2.0	Lisa Cherry	Lee Kelly	Dec 2019	Dec 2020		Yes
	24. Code of Business Standards	7	Lisa Cherry	Lee Kelly	Jun 2020	Jan 2022		Yes
	25. Equality Diversity & Inclusion Policy	2.0	Lisa Cherry	Steve O'Reilly	Nov 2018	Nov 2020		Yes
Finance	26. Post Office Treasury Policy		Alisdair Cameron	Mark Dixon	March 2020	March 2021	RCC & ARC	Yes

DRAFT

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

Policy Paper Appendix C

DRAFT

POL00401629

1. Contract Execution Policy

Policy GE Sponsor	Policy Owner	Contact details	Review history
Ben Foat	Rebecca Whibley	GRO	September 2019

1.1 Purpose and Content of the Policy

The Policy has been established to set out the requirements for execution of contracts in the Group. Such documents should not be executed without the appropriate governance procedures being followed (where applicable), the Policy outlines that in most instances this will be by the completion of the Contract Approval Process and stipulates that no individual should sign a contract who is not an authorised signatory, the Company Secretariat retain a list of authorised signatories.

The Board of each Group Company has authorised specified individuals and/or roles (known as "authorised signatories") to sign contracts on behalf of the respective company. Only these individuals are permitted to sign contracts on behalf of the company. If an unauthorised signatory signs a contract, this must be recorded as a breach of process on the respective company's risk register.

The Policy sets out the following appropriate methods of execution of contracts by authorised signatories within the Group and the requirements and controls for each method.

- Wet Signatures - A wet signature is a handwritten signature by the individual on a hard copy contract
- Electronic Signatures - An electronic signature is "data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign"
- Execution of Deeds - Deeds require a particular method of execution in order to be valid. The Company Secretariat is responsible for the execution of deeds and no deeds should be signed without first consulting the Company Secretariat.

1.2 Key definition

An executed contract is a legal document that has been signed off by the people necessary for it to become effective and therefore the **"Contract Execution"** is the process of signing an agreed contract, after which its terms become binding on the parties to the contract".

1.3 Who Must Comply

All Post Office employees and applies wherever in the world the Group's business is undertaken. All external parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or with their own equivalent policy.

1.4 Key Laws and Regulations

The Group seeks to comply with all relevant UK legislation and regulatory requirements, including but not limited to:

I. Common law
II. Companies Act 2006, specifically ss. 43 – 44

POL00401629

III. General Data Protection Regulation (2016/679 EU) and UK Data Protection Act 2018
IV. Electronic Communications Act 2000)
V. Regulation (EU) No 910/2014 ("eIDAS Regulation")
VI. Privacy and Electronic Communications Regulations 2003

1.5Risk Appetite and Minimum Control Standards

The Group is exposed to a number of risks relating to Contract Execution and the Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group have an Averse risk appetite towards Contract Execution.

The policy outlines minimum control standards across 4 areas of risk. Below is an example of the relationships between the risk area and the required minimum control standards to meet the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Data Security	Sensitive commercial data could be leaked.	Electronic signatures will be managed through software which meets our Information Security standards. - Transmissions to authorised signatories will be encrypted within the software. - Visibility of access to documents is a core component of software functionality and records an audit trail. - Password controls on user access rights to prevent unintended delegation or authorisation.	Information Protection Assurance Team	As appropriate

POL00401629

Contract Execution

Version – V0.2

DRAFT

12

POL00401629

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Application 3
1.4. Authorised Signatories 3
1.5. Methods of Execution 3
1.7. The Risk 6
1.8. Legislation 7
2. Risk Appetite and Minimum Control Standards 8
2.1. Risk Appetite 8
2.2. Policy Framework 8
2.3. Who must comply? 9
2.4. Minimum Control Standards 10
3. Tools & Definitions 13
3.1. Tools 13
3.2. Definitions 13
4. Where to go for help 15
4.1. Additional Policies 15
https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx ..... **Error! Bookmark not defined.**
4.2. How to raise a concern 15
4.3. Who to contact for more information 15
5. Governance 16
5.1. Governance Responsibilities 16
6. Appendix 1: Governance Procedures ..... **Error! Bookmark not defined.**
7. Control 18
7.1. Policy Version 18
7.2. Policy Approval 18
Company Details 19

DRAFT

12

POL00401629

1. Overview

1.1. Introduction by the Policy Owner

The Company Secretariat has overall accountability to the Board of Directors (in each entity within the Post Office group of companies (the **Group**))[1] for the execution of contracts[2] to ensure that the requisite due diligence and oversight is in place prior to signature.

1.2. Purpose

This policy sets out the requirements for execution of contracts in the Group. Such documents should not be executed without the appropriate governance procedures being followed (where applicable).[3] Compliance with this policy will support both individuals and Post Office to be better protected from any legal action.

Every employee has a responsibility to understand the requirements set out in this policy. If there is any misunderstanding, the employee must gain clarification from their line manager.

1.3. Application

This policy is applicable to all employees[4] within the Group.

1.4. Authorised Signatories

The Board of each Group Company has authorised specified individuals and/or roles (known as "authorised signatories") to sign contracts on behalf of the respective company. Only these individuals are permitted to sign contracts on behalf of the company.[5] The Company Secretariat holds the list of authorised signatories for each Group company.

Authorised signatories are only permitted to sign contracts provided the required governance has been completed prior to signature. In most cases this will be the completion of the Contract Approval Process.

1.5. Methods of Execution

The following sets out the appropriate methods of execution of contracts by authorised signatories within the Group and the requirements for each method:

DRAFT

12

---

[1] In this policy "Post Office" and "Group" mean Post Office Limited, Post Office Management Services Limited (Post Office Insurance) and Payzone Bill Payments Limited. First Rate Exchange Services Holdings Limited/ First Rate Exchange Services Limited are not governed by this policy.

[2] Contracts for the purposes of this policy include any legally binding agreement.

[3] See Appendix 1 for Applicable Governance Procedures.

[4] For the purpose of this policy 'employee' means permanent employees, temporary employees (including agency) contractors, consultants and anyone else working on behalf of the Post Office Group.

[5] See Appendix 1 for rules relating to NDAs.

POL00401629

1.5.1. Execution of Contracts

Permitted Method	Explanation	Specific Exclusions	Type of contract	Considerations
Wet signature	Handwritten signature by the individual on a hard copy contract.	• A scanned signature; [6] • An image or photograph of a handwritten signature; or • A *per procurationem* signature (pp.).	Any	The business is responsible for ensuring the external party/ies provides a hard copy signed contract.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. For the purposes of this policy, this means Simple Electronic Signature only[7] via recognised e-signature software.	• Typing a name into the signature block; • pasting an image of a signature into the signature block; • a scanned signature; or • using a finger, light pen or stylus on a touchscreen to write a name electronically into the signature block.[8]	Any, except powers of attorney, trusts, documents submitted to the Land Registry and any documents requiring a signature to be witnessed.	• Ensure that the use of an electronic signature will be legal and enforceable in the context of each individual contract, depending on its governing law. • The Group cannot insist on an external party signing an agreement via electronic signature. • Industry best practice advocates: ○ **Authentication** of the identity of the signatory. ○ **Awareness and intent** to sign - ensuring signatories know and understand they are signing. ○ **Proof** of signing – ensure you can prove a specific document was signed and hasn't been altered since signing. ○ **Consent** – ensure parties have consented to do business

DRAFT

[6] Where *urgent* execution is required and electronic signatures cannot be used, a scanned signature may be accepted if authorised by the Group Company Secretary and wet signed contract must still be provided as soon as possible after execution.

[7] It does not deal with virtual signing (see definitions section 3.2), Advanced Electronic Signature (AdES) or Qualified Electronic Signature.

[8] This does not include approved e-signature software that requires a user to electronically write their name in the system.

POL00401629

				electronically. The work flow of e-signature tools includes an explicit consent. Parties should consider explicitly acknowledging electronic execution in the body of the legal instrument. ○ **Retention** - Keeping good electronic records of all contracts signed electronically. ○ Adherence to Post Office **IT Security Standards**.

1.5.2. Execution of Deeds

Deeds require a particular method of execution in order to be valid. The Company Secretariat is responsible for the execution of deeds and no deeds should be signed without first consulting the Company Secretariat.

Deeds may be signed by electronic signature, provided the other counterparty/ies agree(s) to such a method of execution. The following must be adhered to:

- the business should obtain agreement by email from the other counterparty/ies to sign electronically, as well as lay out the process, and this email should be provided to the Company Secretariat[9]; and
- signature should be by two directors or a director and the company secretary.[10]

The acceptable method of signature varies in accordance to the company:

Company	**Preferred Method of Execution**
Post Office Limited	Affixing the Company Seal, attested by a person authorised to attest the seal; OR Electronic signature by two directors[11] or a director and the company secretary; OR Electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[12]
Post Office Management Services Limited	

12

[9] In property transactions, the external lawyer for the Post Office working on the transaction is to provide evidence of the agreement.

[10] If the counterparty cannot execute in this way, execution may be by a director and witness. The witness must be physically present when the director signs the deed.

[11] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[12] This method of signature is only acceptable where all other methods of signature are not possible.

POL00401629

Payzone Bill Payments Limited	Wet or electronic signature by two directors[13] or a director and the company secretary; OR Wet or electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[14].

1.6. Exceptions

In the ordinary course of events standard business procedures should be followed to ensure that Post Office stays within its defined risk appetite. However, there are situations where business requirements make it necessary to depart from approved policy and take an informed decision to operate outside risk appetite. In these exceptional circumstances, a 'risk exception' can be granted subject to the risk exception process. For more information please contact the Enterprise Risk team for Post Office Limited or the relevant Risk Team for Payzone Bill Payments LimitedPost Office Insurance does not permit exceptions to its approved policies.

1.7. Breaches

A breach of this policy would include:

- where a contract has been signed by an unauthorised signatory from the relevant Group Company;
- where a contract has been signed without first completing the Contract Approval Process (where required); or
- where a contract is signed using the incorrect method of execution as detailed in this policy.

In the event there is a breach of this policy, the incident must be recorded on the respective company's breach register. Where possible, the breach must be remediated and the remediation recorded (for example, the contract is signed again by an authorised signatory and/or by the correct execution method and the previous copy is disregarded). Where the breach cannot be remediated (usually due to the passage of time), the breach must be recorded on the respective company's risk register. Where a breach cannot be remediated, the business must ask Legal to review the contract and the exposure to the Group Company.[15]

The Company Secretariat will advise when such a breach must be reported and to whom it must be reported in conjunction with the relevant company's Risk Team.

1.8. The Risk

All contracts must be signed by an authorised signatory following the completion of the relevant governance process. If this is not followed, there is a risk that the company enters into contracts without proper scrutiny which could open the company up to significant financial loss.

[13] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[14] This method of signature is only acceptable where all other methods of signature are not possible.

[15] Legal may propose an amendment to limit exposure. Such an amendment must be executed in accordance with this policy and would constitute remediation of the initial breach.

POL00401629

An electronic signature must be executed in accordance with paragraph 1.5 to ensure the risk of repudiation is minimal. In the event this cannot be proved, the validity of the signature could be questioned and could prove inadmissible if challenged before a court.

Information within agreements may contain sensitive competitive commercial data or personal information from individuals, such as our customers, colleagues postmasters and business partners, and we need to use this in accordance with relevant legislation (paragraph 1.9), the Policy Framework (paragraph 2.2) and minimum controls standards (paragraph 2.4).

1.9. Legislation

The Group seeks to comply with all relevant UK legislation and regulatory requirements, including but not limited to:

- Common law
- Companies Act 2006, specifically ss. 43 – 44
- General Data Protection Regulation (2016/679 EU) and UK Data Protection Act 2018
- Electronic Communications Act 2000)
- Regulation (EU) No 910/2014 ("eIDAS Regulation")
- Privacy and Electronic Communications Regulations 2003

DRAFT

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group is willing and able to tolerate. The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards.
- **Averse risk appetite** for inefficient or ineffective processes that result in: lost time, duplicated effort, and increased risk of financial losses or errors in any part of its business or core processes.
- **Averse risk appetite** for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed risk appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established a suite of key policies on a risk sensitive approach which are subject to an annual review. The policy suite has been developed to comply with applicable legislation and regulation. The suite of documents pertinent to this policy include:

- **Cyber and Security Information Policy**: A set of high level business principles and activities to protect and assure Post Office's information assets, including critical business information systems, against compromise, unauthorised change, unavailability, loss, damage and destruction.
- **Acceptable Use Standard**: Supports the Cyber and Security Information Policy and governs the fair and acceptable use of Post Office's information assets.
- **Protecting Personal Data Policy**: Requirements of Post Office employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of personal data.
- **Code of Business Standards**: Our Business Standards set out Post Office's vision when dealing with customers, clients and colleagues. The Code explains our key individual responsibilities and how to behave to make Post Office a success.
- **Contract Management Framework:** A clear and standardised management, risk and governance framework that must be complied with in order to achieve effective management of contracts and suppliers and clients.

DRAFT

POL00401629

- **Procurement Policy:** Requirements that must be adhered to when procuring goods and/or services from external suppliers (each Group company must adhere to its own Policy as appropriate).

- **Risk Management Framework:** Comprising (i) the Risk Architecture (i.e. roles, responsibilities, communication and risk reporting arrangements), (ii) the Risk Protocols (i.e. rules and procedures, methodologies, tools and techniques) and (iii) the Risk Strategy (i.e. appetite and attitude to Risk) (as applicable to each Group company).

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All external parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or with their own equivalent policy.

Where non-compliance is identified the matter must be referred to the policy owner. Any investigations will be carried out in accordance with the Investigations Policy. Where it is identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

DRAFT

POL00401629

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined risk appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Unauthorised signatories signing contractual documents, including electronically.	The company is entered into a legally binding agreement or obligation without internal approvals and independent oversight.	Only the Company Secretariat can distribute contractual documents for signature (including via e-signature software). • Process: All contract signatures must be facilitated by the Secretariat and supported by a relevant internal authority evidenced in a Contract Approval Form "CAF" unless a written exception has been agreed by the Company Secretary (e.g. Employment Contracts facilitated by HR, Network Agreements facilitated by the Retail & Franchise Network Team or Standard Non-Disclosure Agreements which may be facilitated by the business). • Assurance: The submission of CAF in accordance with the contract approval process will satisfy the spend approval limits approved by the Board and maintained by the Company Secretary. • Oversight: Only authorised signatories who are not also signatories to the relevant	Company Secretariat All Employees Company Secretariat	Always Always Always

DRAFT

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		CAF (to prevent a conflict of interest) will be requested to sign agreements unless a written exception has been agreed by the Company Secretary. • The list of authorised signatories is maintained by the Company Secretary following Board approval. • Training: Guidance on the company intranet page(s) is updated regularly to provide the business with accurate information on the contract approval and execution processes, including the authorised signatories. • Awareness: Twice yearly communications will be sent to all colleagues to remind them about governance processes and procedures, including authorised signatories.		Annual Board approval Ad hoc updates triggered by changes. Bi-annual review of intranet to check relevance. Bi-annual comms plan
Software Use	Post Office could be fined for using electronic signature software that is not licensed.	Administrators must always be aware of licensing implications and not breach copyright. • Administrators must ensure installations are authorised from Post Office. • Employees must never alter settings within any software as installed, especially security software such as anti-virus. • Employees must never break copyright rules.	Every Employee	As appropriate

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Data Security	Sensitive commercial data could be leaked.	Electronic signatures will be managed through software which meets our Information Security standards. • Transmissions to authorised signatories will be encrypted within the software. • Visibility of access to documents is a core component of software functionality and records an audit trail. • Password controls on user access rights to prevent unintended delegation or authorisation.	Information Protection Assurance Team	As appropriate
Execution of agreements is not binding on parties	Developments in common law / statute could change the legal basis for execution.	Policy review will be carried out on an annual basis and can be triggered sooner by a material legislative change.	Company Secretariat	Annual

DRAFT

POL00401629

3. Tools & Definitions

3.1. Tools

1. The Group has procured an approved e-signature solution.
2. Group authorised signatories are trained to understand the contract execution process, only recognise requests from the Company Secretariat and to require evidence of explicit consent (e.g. the CAF) to do business before engaging in the signature process. Consent to electronically sign documents is built into the workflow of the approved e-signature solution.

3.2. Definitions

1. **Wet signature**: Handwritten signature by an individual on an original hard copy document.
2. **Seal**: Company seal of the Company recognised under the company's Articles of Association.
3. **Deed**: A written document which is executed with the necessary formality (more than a simple signature), and by which an interest, right or property passes or is confirmed, or an obligation binding on some person is created or confirmed.
4. **Electronic signature** or **e-signature**: "Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign".[16] For the purposes of this policy, the Group position is that this does not include the situations listed in section 1.4 (a-d).
5. **Contract Approval Process**: Internal governance process that must be completed prior to the execution of an agreement with an external party (excluding employment and agency contracts managed by HR). Guidance on the contract approval process is available via the intranet. If you are unsure whether an eCAF is required prior to contract execution, please email your query to caf: GRO
6. **Contract Approval Form (CAF) or eCAF**: The form used to complete the Contract Approval Process. This form requires sign offs from the relevant stakeholders within the business. This form[17] can be found on the Company Secretariat intranet page.
7. **Virtual signing**: This refers to when a document is signed without all the parties being physically present at the same meeting.
8. **Delegated Authorities**: The relevant Board of Directors delegates its authority to enter into contracts with external parties to various colleagues within the Group,

12

[16] Regulation (EU) No 910/2014 ("eIDAS Regulation") Article 3(10)

[17] For Post Office Limited, this form is completed online in the Contract Approval Form App. For other companies in the Group, the Word document form must be completed.

POL00401629

according to specified financial limits. An up-to-date list of the delegated authorities can be found on the Company Secretariat intranet page.

9. **Authorised Signatory**: The relevant Board of Directors has specified a list of individuals who are authorised to sign legally binding agreements on behalf of the Group. The Company Secretariat arrange for the signature of all agreements, save for employment and agency/network contracts, to ensure only an authorised signatory is used.

10. **Tolerant Risk:** Risk appetite approach where Post Office is willing to (i) take greater than normal risks (ii) accept some negative impact in order to pursue objective (iii) accept some residual risk.

11. **Averse Risk**: Risk appetite approach where Post Office (i) actively discourages risk taking (ii) is not willing to accept any negative impact (iii) will mitigate or treat risks in order to minimise residual risk.

12. **Standard Non-Disclosure Agreement** (NDA): This is used when parties wish to share and exchange confidential information. The Post Office Legal Team has drafted and approved a Post Office House Position for NDAs. Where the House Position template is used, no changes should be made to the contract (outside of the guidance to the template). This type of NDA does not require a CAF.

13. **Non-standard Non-Disclosure Agreement** (NDA): This is either a standard NDA which has been amended outside the House Position detailed above or a NDA which is entirely different to the standard template, such as an NDA provided by an external party. This type of NDA requires a CAF.

DRAFT

POL00401629

4. Where to go for help

4.1. Additional Policies

All Key Policies are found on the Hub intranet page.

4.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO.
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Company Secretariat: GRO

DRAFT

12

POL00401629

5. Governance

5.1. Governance Responsibilities

The policy sponsor, responsible for overseeing this policy is the Group General Counsel of Post Office Group.

The policy owner is the Group Company Secretary who is responsible for ensuring that the Company Secretariat conducts an annual review of this policy and tests compliance across the Group. Additionally the Group Company Secretary is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit, Risk and Compliance Committee where appropriate.

The relevant Board is responsible for setting the Post Office's risk appetite.

Each Board of Directors may delegate its authority in accordance with the company's Articles of Association. Authorised signatories are approved by the Board of Directors. The Company Secretariat maintains a list of spend approval limits and list of authorised signatories approved by the relevant Board.

5.2. Governance Procedures

5.2.1. Contract Approval Process

Prior to execution, all contracts must have been approved via the appropriate governance procedures.

The Contract Approval Process is applicable to all contracts, except:

- Employment Contracts;
- Network/Agency Contracts;
- Standard Non-Disclosure Agreements (NDA); and
- Property Contracts.

In all other cases, the Contract Approval Process must be completed prior to contract signature. Guidance on the contract approval process is available via the intranet. If you are unsure whether you need to complete the Contract Approval Process, please email your query to caf[redacted].

5.2.2. Exceptions to the Contract Approval Process

5.2.2.1. Employment & Network Contracts

These contracts are managed by the HR and Network teams respectively. The internal governance required within those teams must be completed prior to contract signature. Only certain individuals within these teams are authorised to sign such contracts and this list is held by the Company Secretariat.

DRAFT

POL00401629

5.2.2.2. Non-Disclosure Agreements

If using a standard NDA, the Contract Approval Process need not be followed and the agreement may be signed by any individual in the business. A copy should still be provided to the Company Secretariat.

If using a non-standard NDA, the Contract Approval Process must be completed in the normal way and the contract signed by an authorised signatory in accordance with this policy.

5.2.2.3. Property Contracts

These contracts are managed by the Property & Legal team and their governance procedures must be followed prior to contract execution. Contract execution is managed by the Company Secretariat in accordance with this policy.

DRAFT

POL00401629

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
22.08.2019	0.1	Policy Author	Draft Version
01.09.2020	0.2	Policy Author	Streamlining of acceptable methods of execution section Addition of signing deeds electronically Process for urgent signature by scanned signature Clarification of exceptions and breach process for all Group Companies Minor language amendments Updated the oversight committee

6.2. Policy Approval

Group Oversight Committee: Audit & Risk Committee

Committee	Date Approved
POL R&CC	
POL ARC	
POMS R&CC	
PZBPL Board	

Policy Sponsor: Ben Foat, Group General Counsel
Policy Owner: Veronica Branton, Group Company Secretary
Policy Author: Rebecca Whibley, Assistant Company Secretary
Next review: .2021

DRAFT

POL00401629

Company Details

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

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

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

Payzone Bill Payments Limited is registered in England and Wales. Registered number 11310918. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

DRAFT

POL00401629

Contract Execution

Version – V0.2

DRAFT

12

POL00401629

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Application 3
1.4. Authorised Signatories 3
1.5. Methods of Execution 3
1.7. The Risk 6
1.8. Legislation 7
2. Risk Appetite and Minimum Control Standards 8
2.1. Risk Appetite 8
2.2. Policy Framework 8
2.3. Who must comply? 9
2.4. Minimum Control Standards 10
3. Tools & Definitions 13
3.1. Tools 13
3.2. Definitions 13
4. Where to go for help 15
4.1. Additional Policies 15
https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx ..... **Error! Bookmark not defined.**
4.2. How to raise a concern 15
4.3. Who to contact for more information 15
5. Governance 16
5.1. Governance Responsibilities 16
6. Appendix 1: Governance Procedures ..... **Error! Bookmark not defined.**
7. Control 18
7.1. Policy Version 18
7.2. Policy Approval 18
Company Details 19

DRAFT

POL00401629

1. Overview

1.1. Introduction by the Policy Owner

The Company Secretariat has overall accountability to the Board of Directors (in each entity within the Post Office group of companies (the **Group**))[1] for the execution of contracts[2] to ensure that the requisite due diligence and oversight is in place prior to signature.

1.2. Purpose

This policy sets out the requirements for execution of contracts in the Group. Such documents should not be executed without the appropriate governance procedures being followed (where applicable).[3] Compliance with this policy will support both individuals and Post Office to be better protected from any legal action.

Every employee has a responsibility to understand the requirements set out in this policy. If there is any misunderstanding, the employee must gain clarification from their line manager.

1.3. Application

This policy is applicable to all employees[4] within the Group.

1.4. Authorised Signatories

The Board of each Group Company has authorised specified individuals and/or roles (known as "authorised signatories") to sign contracts on behalf of the respective company. Only these individuals are permitted to sign contracts on behalf of the company.[5] The Company Secretariat holds the list of authorised signatories for each Group company.

Authorised signatories are only permitted to sign contracts provided the required governance has been completed prior to signature. In most cases this will be the completion of the Contract Approval Process.

1.5. Methods of Execution

The following sets out the appropriate methods of execution of contracts by authorised signatories within the Group and the requirements for each method:

DRAFT

12

---

[1] In this policy "Post Office" and "Group" mean Post Office Limited, Post Office Management Services Limited (Post Office Insurance) and Payzone Bill Payments Limited. First Rate Exchange Services Holdings Limited/ First Rate Exchange Services Limited are not governed by this policy.

[2] Contracts for the purposes of this policy include any legally binding agreement.

[3] See Appendix 1 for Applicable Governance Procedures.

[4] For the purpose of this policy 'employee' means permanent employees, temporary employees (including agency) contractors, consultants and anyone else working on behalf of the Post Office Group.

[5] See Appendix 1 for rules relating to NDAs.

POL00401629

1.5.1. Execution of Contracts

Permitted Method	Explanation	Specific Exclusions	Type of contract	Considerations
Wet signature	Handwritten signature by the individual on a hard copy contract.	• A scanned signature; [6] • An image or photograph of a handwritten signature; or • A *per procurationem* signature (pp.).	Any	The business is responsible for ensuring the external party/ies provides a hard copy signed contract.
Electronic signature	Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign. For the purposes of this policy, this means Simple Electronic Signature only[7] via recognised e-signature software.	• Typing a name into the signature block; • pasting an image of a signature into the signature block; • a scanned signature; or • using a finger, light pen or stylus on a touchscreen to write a name electronically into the signature block.[8]	Any, except powers of attorney, trusts, documents submitted to the Land Registry and any documents requiring a signature to be witnessed.	• Ensure that the use of an electronic signature will be legal and enforceable in the context of each individual contract, depending on its governing law. • The Group cannot insist on an external party signing an agreement via electronic signature. • Industry best practice advocates: ○ **Authentication** of the identity of the signatory. ○ **Awareness and intent** to sign - ensuring signatories know and understand they are signing. ○ **Proof** of signing – ensure you can prove a specific document was signed and hasn't been altered since signing. ○ **Consent** – ensure parties have consented to do business

DRAFT

[6] Where *urgent* execution is required and electronic signatures cannot be used, a scanned signature may be accepted if authorised by the Group Company Secretary and wet signed contract must still be provided as soon as possible after execution.

[7] It does not deal with virtual signing (see definitions section 3.2), Advanced Electronic Signature (AdES) or Qualified Electronic Signature.

[8] This does not include approved e-signature software that requires a user to electronically write their name in the system.

POL00401629

				electronically. The work flow of e-signature tools includes an explicit consent. Parties should consider explicitly acknowledging electronic execution in the body of the legal instrument. ○ **Retention** - Keeping good electronic records of all contracts signed electronically. ○ Adherence to Post Office **IT Security Standards**.

1.5.2. Execution of Deeds

Deeds require a particular method of execution in order to be valid. The Company Secretariat is responsible for the execution of deeds and no deeds should be signed without first consulting the Company Secretariat.

Deeds may be signed by electronic signature, provided the other counterparty/ies agree(s) to such a method of execution. The following must be adhered to:

- the business should obtain agreement by email from the other counterparty/ies to sign electronically, as well as lay out the process, and this email should be provided to the Company Secretariat[9]; and
- signature should be by two directors or a director and the company secretary.[10]

The acceptable method of signature varies in accordance to the company:

Company	**Preferred Method of Execution**
Post Office Limited	Affixing the Company Seal, attested by a person authorised to attest the seal; OR Electronic signature by two directors[11] or a director and the company secretary; OR Electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[12]
Post Office Management Services Limited	

[9] In property transactions, the external lawyer for the Post Office working on the transaction is to provide evidence of the agreement.

[10] If the counterparty cannot execute in this way, execution may be by a director and witness. The witness must be physically present when the director signs the deed.

[11] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[12] This method of signature is only acceptable where all other methods of signature are not possible.

POL00401629

Payzone Bill Payments Limited	Wet or electronic signature by two directors[13] or a director and the company secretary; OR Wet or electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[14].

1.6. Exceptions

In the ordinary course of events standard business procedures should be followed to ensure that Post Office stays within its defined risk appetite. However, there are situations where business requirements make it necessary to depart from approved policy and take an informed decision to operate outside risk appetite. In these exceptional circumstances, a 'risk exception' can be granted subject to the risk exception process. For more information please contact the Enterprise Risk team for Post Office Limited or the relevant Risk Team for Payzone Bill Payments LimitedPost Office Insurance does not permit exceptions to its approved policies.

1.7. Breaches

A breach of this policy would include:

- where a contract has been signed by an unauthorised signatory from the relevant Group Company;
- where a contract has been signed without first completing the Contract Approval Process (where required); or
- where a contract is signed using the incorrect method of execution as detailed in this policy.

In the event there is a breach of this policy, the incident must be recorded on the respective company's breach register. Where possible, the breach must be remediated and the remediation recorded (for example, the contract is signed again by an authorised signatory and/or by the correct execution method and the previous copy is disregarded). Where the breach cannot be remediated (usually due to the passage of time), the breach must be recorded on the respective company's risk register. Where a breach cannot be remediated, the business must ask Legal to review the contract and the exposure to the Group Company.[15]

The Company Secretariat will advise when such a breach must be reported and to whom it must be reported in conjunction with the relevant company's Risk Team.

1.8. The Risk

All contracts must be signed by an authorised signatory following the completion of the relevant governance process. If this is not followed, there is a risk that the company enters into contracts without proper scrutiny which could open the company up to significant financial loss.

[13] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[14] This method of signature is only acceptable where all other methods of signature are not possible.

[15] Legal may propose an amendment to limit exposure. Such an amendment must be executed in accordance with this policy and would constitute remediation of the initial breach.

POL00401629

An electronic signature must be executed in accordance with paragraph 1.5 to ensure the risk of repudiation is minimal. In the event this cannot be proved, the validity of the signature could be questioned and could prove inadmissible if challenged before a court.

Information within agreements may contain sensitive competitive commercial data or personal information from individuals, such as our customers, colleagues postmasters and business partners, and we need to use this in accordance with relevant legislation (paragraph 1.9), the Policy Framework (paragraph 2.2) and minimum controls standards (paragraph 2.4).

1.9. Legislation

The Group seeks to comply with all relevant UK legislation and regulatory requirements, including but not limited to:

- Common law
- Companies Act 2006, specifically ss. 43 – 44
- General Data Protection Regulation (2016/679 EU) and UK Data Protection Act 2018
- Electronic Communications Act 2000)
- Regulation (EU) No 910/2014 ("eIDAS Regulation")
- Privacy and Electronic Communications Regulations 2003

DRAFT

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group is willing and able to tolerate. The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality.
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards.
- **Averse risk appetite** for inefficient or ineffective processes that result in: lost time, duplicated effort, and increased risk of financial losses or errors in any part of its business or core processes.
- **Averse risk appetite** for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed risk appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established a suite of key policies on a risk sensitive approach which are subject to an annual review. The policy suite has been developed to comply with applicable legislation and regulation. The suite of documents pertinent to this policy include:

- **Cyber and Security Information Policy**: A set of high level business principles and activities to protect and assure Post Office's information assets, including critical business information systems, against compromise, unauthorised change, unavailability, loss, damage and destruction.
- **Acceptable Use Standard**: Supports the Cyber and Security Information Policy and governs the fair and acceptable use of Post Office's information assets.
- **Protecting Personal Data Policy**: Requirements of Post Office employees and third parties in relation to the collection, use, retention, transfer, disclosure and destruction of personal data.
- **Code of Business Standards**: Our Business Standards set out Post Office's vision when dealing with customers, clients and colleagues. The Code explains our key individual responsibilities and how to behave to make Post Office a success.
- **Contract Management Framework:** A clear and standardised management, risk and governance framework that must be complied with in order to achieve effective management of contracts and suppliers and clients.

DRAFT

POL00401629

- **Procurement Policy:** Requirements that must be adhered to when procuring goods and/or services from external suppliers (each Group company must adhere to its own Policy as appropriate).

- **Risk Management Framework:** Comprising (i) the Risk Architecture (i.e. roles, responsibilities, communication and risk reporting arrangements), (ii) the Risk Protocols (i.e. rules and procedures, methodologies, tools and techniques) and (iii) the Risk Strategy (i.e. appetite and attitude to Risk) (as applicable to each Group company).

2.3. Who must comply?

Compliance with this policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All external parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or with their own equivalent policy.

Where non-compliance is identified the matter must be referred to the policy owner. Any investigations will be carried out in accordance with the Investigations Policy. Where it is identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

DRAFT

POL00401629

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined risk appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Unauthorised signatories signing contractual documents, including electronically.	The company is entered into a legally binding agreement or obligation without internal approvals and independent oversight.	Only the Company Secretariat can distribute contractual documents for signature (including via e-signature software). • Process: All contract signatures must be facilitated by the Secretariat and supported by a relevant internal authority evidenced in a Contract Approval Form "CAF" unless a written exception has been agreed by the Company Secretary (e.g. Employment Contracts facilitated by HR, Network Agreements facilitated by the Retail & Franchise Network Team or Standard Non-Disclosure Agreements which may be facilitated by the business). • Assurance: The submission of CAF in accordance with the contract approval process will satisfy the spend approval limits approved by the Board and maintained by the Company Secretary. • Oversight: Only authorised signatories who are not also signatories to the relevant	Company Secretariat All Employees Company Secretariat	Always Always Always

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		CAF (to prevent a conflict of interest) will be requested to sign agreements unless a written exception has been agreed by the Company Secretary. • The list of authorised signatories is maintained by the Company Secretary following Board approval. • Training: Guidance on the company intranet page(s) is updated regularly to provide the business with accurate information on the contract approval and execution processes, including the authorised signatories. • Awareness: Twice yearly communications will be sent to all colleagues to remind them about governance processes and procedures, including authorised signatories.		Annual Board approval Ad hoc updates triggered by changes. Bi-annual review of intranet to check relevance. Bi-annual comms plan
Software Use	Post Office could be fined for using electronic signature software that is not licensed.	Administrators must always be aware of licensing implications and not breach copyright. • Administrators must ensure installations are authorised from Post Office. • Employees must never alter settings within any software as installed, especially security software such as anti-virus. • Employees must never break copyright rules.	Every Employee	As appropriate

DRAFT

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Data Security	Sensitive commercial data could be leaked.	Electronic signatures will be managed through software which meets our Information Security standards. • Transmissions to authorised signatories will be encrypted within the software. • Visibility of access to documents is a core component of software functionality and records an audit trail. • Password controls on user access rights to prevent unintended delegation or authorisation.	Information Protection Assurance Team	As appropriate
Execution of agreements is not binding on parties	Developments in common law / statute could change the legal basis for execution.	Policy review will be carried out on an annual basis and can be triggered sooner by a material legislative change.	Company Secretariat	Annual

DRAFT

POL00401629

3. Tools & Definitions

3.1. Tools

1. The Group has procured an approved e-signature solution.
2. Group authorised signatories are trained to understand the contract execution process, only recognise requests from the Company Secretariat and to require evidence of explicit consent (e.g. the CAF) to do business before engaging in the signature process. Consent to electronically sign documents is built into the workflow of the approved e-signature solution.

3.2. Definitions

1. **Wet signature**: Handwritten signature by an individual on an original hard copy document.
2. **Seal**: Company seal of the Company recognised under the company's Articles of Association.
3. **Deed**: A written document which is executed with the necessary formality (more than a simple signature), and by which an interest, right or property passes or is confirmed, or an obligation binding on some person is created or confirmed.
4. **Electronic signature** or **e-signature**: "Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign".[16] For the purposes of this policy, the Group position is that this does not include the situations listed in section 1.4 (a-d).
5. **Contract Approval Process**: Internal governance process that must be completed prior to the execution of an agreement with an external party (excluding employment and agency contracts managed by HR). Guidance on the contract approval process is available via the intranet. If you are unsure whether an eCAF is required prior to contract execution, please email your query to caf: GRO
6. **Contract Approval Form (CAF) or eCAF**: The form used to complete the Contract Approval Process. This form requires sign offs from the relevant stakeholders within the business. This form[17] can be found on the Company Secretariat intranet page.
7. **Virtual signing**: This refers to when a document is signed without all the parties being physically present at the same meeting.
8. **Delegated Authorities**: The relevant Board of Directors delegates its authority to enter into contracts with external parties to various colleagues within the Group,

12

[16] Regulation (EU) No 910/2014 ("eIDAS Regulation") Article 3(10)

[17] For Post Office Limited, this form is completed online in the Contract Approval Form App. For other companies in the Group, the Word document form must be completed.

POL00401629

according to specified financial limits. An up-to-date list of the delegated authorities can be found on the Company Secretariat intranet page.

9. **Authorised Signatory**: The relevant Board of Directors has specified a list of individuals who are authorised to sign legally binding agreements on behalf of the Group. The Company Secretariat arrange for the signature of all agreements, save for employment and agency/network contracts, to ensure only an authorised signatory is used.

10. **Tolerant Risk:** Risk appetite approach where Post Office is willing to (i) take greater than normal risks (ii) accept some negative impact in order to pursue objective (iii) accept some residual risk.

11. **Averse Risk**: Risk appetite approach where Post Office (i) actively discourages risk taking (ii) is not willing to accept any negative impact (iii) will mitigate or treat risks in order to minimise residual risk.

12. **Standard Non-Disclosure Agreement** (NDA): This is used when parties wish to share and exchange confidential information. The Post Office Legal Team has drafted and approved a Post Office House Position for NDAs. Where the House Position template is used, no changes should be made to the contract (outside of the guidance to the template). This type of NDA does not require a CAF.

13. **Non-standard Non-Disclosure Agreement** (NDA): This is either a standard NDA which has been amended outside the House Position detailed above or a NDA which is entirely different to the standard template, such as an NDA provided by an external party. This type of NDA requires a CAF.

DRAFT

POL00401629

4. Where to go for help

4.1. Additional Policies

All Key Policies are found on the Hub intranet page.

4.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: GRO or by telephone on: GRO.
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Company Secretariat: GRO

DRAFT

POL00401629

5. Governance

5.1. Governance Responsibilities

The policy sponsor, responsible for overseeing this policy is the Group General Counsel of Post Office Group.

The policy owner is the Group Company Secretary who is responsible for ensuring that the Company Secretariat conducts an annual review of this policy and tests compliance across the Group. Additionally the Group Company Secretary is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit, Risk and Compliance Committee where appropriate.

The relevant Board is responsible for setting the Post Office's risk appetite.

Each Board of Directors may delegate its authority in accordance with the company's Articles of Association. Authorised signatories are approved by the Board of Directors. The Company Secretariat maintains a list of spend approval limits and list of authorised signatories approved by the relevant Board.

5.2. Governance Procedures

5.2.1. Contract Approval Process

Prior to execution, all contracts must have been approved via the appropriate governance procedures.

The Contract Approval Process is applicable to all contracts, except:

- Employment Contracts;
- Network/Agency Contracts;
- Standard Non-Disclosure Agreements (NDA); and
- Property Contracts.

In all other cases, the Contract Approval Process must be completed prior to contract signature. Guidance on the contract approval process is available via the intranet. If you are unsure whether you need to complete the Contract Approval Process, please email your query to caf[redacted]

5.2.2. Exceptions to the Contract Approval Process

5.2.2.1. Employment & Network Contracts

These contracts are managed by the HR and Network teams respectively. The internal governance required within those teams must be completed prior to contract signature. Only certain individuals within these teams are authorised to sign such contracts and this list is held by the Company Secretariat.

DRAFT

POL00401629

5.2.2.2. Non-Disclosure Agreements

If using a standard NDA, the Contract Approval Process need not be followed and the agreement may be signed by any individual in the business. A copy should still be provided to the Company Secretariat.

If using a non-standard NDA, the Contract Approval Process must be completed in the normal way and the contract signed by an authorised signatory in accordance with this policy.

5.2.2.3. Property Contracts

These contracts are managed by the Property & Legal team and their governance procedures must be followed prior to contract execution. Contract execution is managed by the Company Secretariat in accordance with this policy.

DRAFT

POL00401629

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
22.08.2019	0.1	Policy Author	Draft Version
01.09.2020	0.2	Policy Author	Streamlining of acceptable methods of execution section Addition of signing deeds electronically Process for urgent signature by scanned signature Clarification of exceptions and breach process for all Group Companies Minor language amendments Updated the oversight committee

6.2. Policy Approval

Group Oversight Committee: Audit & Risk Committee

Committee	Date Approved
POL R&CC	
POL ARC	
POMS R&CC	
PZBPL Board	

Policy Sponsor: Ben Foat, Group General Counsel
Policy Owner: Veronica Branton, Group Company Secretary
Policy Author: Rebecca Whibley, Assistant Company Secretary
Next review: .2021

DRAFT

POL00401629

Company Details

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

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

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

Payzone Bill Payments Limited is registered in England and Wales. Registered number 11310918. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

DRAFT

POL00401629

Contract Execution Quick Reference Guide

This document provides a summary of the Contract Execution Policy for quick reference. The full policy may be accessed on the Intranet.

Key Points

- No contract should be executed (signed) without the appropriate governance procedures being followed. In most instances, this will be by the completion of the Contract Approval Process. See the CoSec Intranet Page for more information.
- No individual should sign a contract who is not an authorised signatory.[1] The Company Secretariat retain a list of authorised signatories.
- The below sets out the acceptable methods of execution and the requirements around each method.

Wet Signatures

- Only hard copy, wet signatures are acceptable.
- This does not include: scanned signatures, an image or photograph of a signature; or a *per procurationem* signature (pp.). (*Scanned signatures may be accepted, by exception, if execution is urgent, no other method is possible and the Company Secretary authorises an exception, but a hard copy is still required in due course*).

Electronic Signatures

- The Business must consider whether electronic signatures are appropriate for their contract given the governing law of their contract.
- The Business cannot insist that an external party signs using electronic signatures.
- Electronic signatures must be simple electronic signatures and obtained via approved e-signature software.
- The following methods of signature should not be used nor accepted on legally binding documents:
  i. Typing a name into a signature block;
  ii. Electronic pasting of a signature (i.e. an image of a signature);
  iii. A handwritten signature that is scanned; or
  iv. Using a finger, light pen, or stylus on a touch screen to write a name electronically.
- Electronic signatures should not be used for:
  i. powers of attorney;
  ii. trusts;
  iii. documents which need to be submitted to the Land Registry; and
  iv. any other document that requires a signature to be witnessed.

Deeds

- The acceptable method of signature varies in accordance to the company:

Company	Preferred Method of Execution
Post Office Limited	Affixing the Company Seal, attested by a person authorised to attest the seal; OR Electronic signature by two directors[2] or a director and the company secretary; OR Electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[3]
Post Office Management Services Limited	Wet or electronic signature by two directors[4] or a director and the company secretary; OR Wet or electronic signature by a director in the presence of a witness who attests the signature (a witness who is physically present to witnesses the director e-signing)[5].
Payzone Bill Payments Limited	

[1] The only exception to this is for standard non-disclosure agreements which may be signed by business units and copies provided to the Company Secretariat.

[2] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[3] This method of signature is only acceptable where all other methods of signature are not possible.

[4] Director for the purposes of this policy means statutory director and does not include colleagues whose job title is director.

[5] This method of signature is only acceptable where all other methods of signature are not possible.

12

POL00401629

12

POL00401629

1. Vulnerable Customer Policy

Policy GE Sponsor	Policy Owner	Contact details	Review history
Ben Foat	Paul Beaumont	GRO	September 2019

1.1 Purpose and Content of the Policy

The Vulnerable Customer Policy articulates Post Office's expectations as to how we support vulnerable customers across all our channels and that the operations of Post Office do not have any negative impact upon vulnerable customers.

The policy aims to address that all members of staff who have any customer contact have a duty to help ensure that vulnerable customers are treated fairly and when vulnerability is identified adaptations are made to fully assist.
Addressing the needs of vulnerable customers is core to Post Office's social purpose and is aligned to our objectives to be 'Better for Customers' and a 'Great Place to Work'.

The Policy outlines the core principles of customer vulnerability and emphasis that vulnerability can impact in many ways and can be permanent or temporary.
The Post Office recognises that these customers may have additional needs and may be described as 'vulnerable' although it is important to note that these customers may not regard themselves as such. It is core to Post Office's rationale and purpose to ensure that appropriate respect and care is taken of all types of customer, including vulnerable customers.

The Vulnerable Customer Policy sets out;

- The outcomes employees must achieve for customers;
- A framework for delivering these outcomes, including key controls and putting things right when they go wrong;
- Key examples to think about when assessing what fair treatment means for customers who may be deemed vulnerable

1.2 Key Definition

The FCA **define** a "**vulnerable consumer"** as: 'Someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care'.

12

1.3 Who Must Comply

all Post Office employees. Post Office will work with Agency network, Principals and key commercial partners to ensure that where possible the spirit of our approach to vulnerable customers is applied.

1.4 Key Laws and Regulations

There are a number of relevant UK legal and regulatory requirements which are applicable including (but not limited to):

I. Ofcom duties under the Communications Act
II. Equality Act 2010
III. Mental Capacity Act 2005 and guidance

POL00401629

IV. The Lasting Powers of Attorney, Enduring Powers of Attorney and Public Guardian Regulations 2007
V. Disability Discrimination Act (Northern Ireland) 2005.
VI. Adults with Incapacity (Scotland) Act 2000. ☐ Consumer vulnerability regulation detailed within the FCA Handbook for CONC and Mortgage Conduct of Business (MCOB).
VII. FCA General Guidance on minimum standards 2019

Industry Guidance

I. FCA website including 2016 Thematic Review on vulnerable customers
II. UK Finance ☐ Age UK advice line
III. Money Advice Service
IV. Pensions Advisory Service
V. Alzheimer's Society guidance on Mental Capacity Act provisions Gov.uk
VI. Citizen's Advice Bureau
VII. Ofcom's Fairness Principles
VIII. Ofcom guidelines on Vulnerability

The Department of Business Energy and Industrial Strategy Green paper has the protection of vulnerable customers as a key strategic priority for government. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly.

1.5 Risk Appetite and Minimum Control Standards

Regulators are attaching increasing importance to customer vulnerability, therefore current regulation and legislation regarding customer vulnerability means that the Group needs to have a robust risk approach to vulnerability, including implementing effective policies and procedures to ensure a consistent approach is being taken across the group and operations are clear to mitigate such risks when they arise.

The Group has an Averse Risk Appetite and zero tolerance for:

- Regulatory breaches; or
- unfair customer outcomes arising from product design, sales or after sales processes.

The policy outlines minimum control standards across 2 areas of risk. Below is an example of the relationships between the risk area and the required minimum control standards to meet the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Customer engagement with products and services is not possible or limited because of a vulnerability	**B.** Communications Needs A customer may be particularly vulnerable because they have a hearing or sight impairment, which means	• We will look to make 'reasonable adjustments' to the way in which we are able to com-	All product teams Director Retail Network	Ongoing

POL00401629

	they require specially adapted methods of communication.	municate with our customers. For instance for sight impairment, we will seek to ensure that our customer documentation is available in a range of formats to help them understand our product material and product-life cycle communications.		
		• We will meet the accessibility requirements for Public Sector websites and Apps	Digital Team	Ongoing
		• For hearing impairment, we will seek to provide functioning hearing loops for DMB and provide guidance on where to maintain service loops to the wider Network.	DMB Engineering team	Ongoing

12

POL00401629

Vulnerable Customer Policy

Version –draft (for approval) 3.1

12

POL00401629

Group Oversight Committee:	Audit and Risk Committee
Sign-off Authority:	Risk and Compliance Committee
Policy Sponsor:	Jonathan Hill
Policy Owner:	Paul Beaumont
Policy Author:	Paul Beaumont
Approved by:	Audit and Risk Committee
Approved:	
Next review:	

POL00401629

1. Overview 4
1.1. Introduction by the Policy Owner 4
1.2. Purpose 4
1.3. Core Principles 5
1.4. Application 5
1.5. Risk 7
1.6. Legislation 7
1.7. Industry Guidance 7
2. Risk Appetite and Minimum Control Standards 9
2.1. Risk Appetite 9
2.2. Policy Framework 9
2.3. Who must comply? 9
2.4. Minimum Control Standards 9
3. Where to go for help 15
3.1. Additional Policies 15
3.2. How to raise a concern 15
3.3. Who to contact for more information 15
3.4. Company Details 15

12

POL00401629

1. Overview

1.1. Introduction by the Policy Owner

Significant groups in our communities are impacted either temporarily or permanently by vulnerability. For example;

- There are 850 thousand people in the UK with dementia and this is expected to rise to a million over the next three years (Alzheimer's Society 2018)
- In any given year one in four of the adult population suffers a mental illness (NHS 2017)
- Over 2 million people in the UK are coping with sight loss (RNIB 2019)
- 8.8 million people in the UK have caring responsibilities. (Carers UK 2019)
- There were 2.5 million people living with cancer in 2015. This will rise to 4 million by 2030 (Macmillan 2019)
- One in 6 adults have very poor literacy skills: (National Literacy Trust 2019)
- Just under a half of the population has numeracy attainment skills of a child at primary school (National Numeracy 2017)

At the Post Office we are committed to providing quality products and services for all our customers. We work in an open and responsible way that builds the trust and respect of all our customers. Post Office seeks to ensure that all customers can make good buying decisions and have a positive experience when dealing with us.

Addressing the needs of vulnerable customers is core to Post Office's social purpose and is aligned to our objectives to be 'Better for Customers' and a 'Great Place to Work'. There are countless examples of how we assist customers when they need us most. This policy outlines the policy approach so that we continue to ensure that we are able to look after the needs of vulnerable customers.

1.2. Purpose

To articulate Post Office's expectations as to how we support vulnerable customers across all our channels.

This will also be an important document and source of information on Post Office's policy approach to vulnerable customers for many of our stakeholders.

1.3 Definition

A vulnerable customer is someone who, due to their personal circumstances, is more likely to require additional support to access the services provided by Post Office.

POL00401629

Customers may be vulnerable due to circumstances such as age, physical or learning disability, physical or mental illness, low literacy, communications difficulties or changes in circumstances such as bereavement.

1.4 Core Principles

Vulnerability can impact in many ways and can be permanent or temporary, these categories are examples. The Post Office recognises that these customers may have additional needs and may be described as 'vulnerable' although it is important to note that these customers may not regard themselves as such. It is core to Post Office's rationale and purpose to ensure that appropriate respect and care is taken of all types of customer, including vulnerable customers.

Categories include:

A. Restricted Mobility B. Communications needs including sight and hearing loss C. Low Basic Skills D. Low Financial Capability	E. Mental Capacity F. Age Related Vulnerability G. Life Event Vulnerability e.g., bereavement, critical illness, redundancy H. Financial Difficulties

1.5 Examples

There are already many examples of how Post Office assists vulnerable customers these include:

- POca serves to meet the needs of the most vulnerable in society including the 'unbanked' and 'financially excluded' through facilitating government payments into a cash account with proprietary card access
- During Covid 19 we have developed alternative ways for vulnerable customers to access cash
- Bill payments operates as a key service for vulnerable customers. In particular the unbanked and those financially excluded. Ability to pay bills via the SSK gives vulnerable customers additional support through trained people on hand.
- Numerous examples of community outreach and partnerships with local charities/vulnerable customers made through Agency branches.
- The Banking Framework is a key demonstration of how Post Office is supporting elderly and vulnerable customers. We are increasingly the last 'bank' in town as bank branches close supporting those who prefer to do their banking in branch with the additional support that Post Offices can offer at the counter.
- A Banking process currently exists for vulnerable customers when they are unable to use the chip & Pin functionality.
- Updating our branch accessibility guidance using specialist accessibility consultants
- Working with partners such as BoI who have given forbearance measures under Covid 19 but who also give case by case exceptions to the 'terms of conditions' for vulnerable customers recognising their condition, for

POL00401629

example customers in hospital unable to read banking correspondence and statements, or those that have suffered a bout of mental illness.

- Vulnerable customer training module on Success Factors and further development planned to enhance the Customer Experience Academy.
- In telecoms those who are struggling to pay, can have a new COVID 19 flag added to their account and there are measures in place to help
- In telecoms we have also set up a triage desk to deal with escalated issues. This has involved sending out temporary mobile phones for customers who have a fault on their line which will take a while to fix (e.g. Openreach need to fix a cable that a digger cut through at the exchange) and yet their landline is their lifeline.
- In telecoms we have committed to Ofcom's fairness commitments, which give significant undertakings to support vulnerable customers

1.7 Application

Accessibility Guidance.

The Post Office Health and Safety team provide network accessibility guidance with the help of outside experts. Much of this is based on the current legal requirements particularly the Equality Act. It is the responsibility of staff and Postmasters to ensure that they comply with and observe these requirements, and where there is any uncertainty, to seek clarification from relevant Post Office subject matter experts to ensure compliance. This guidance also provides useful advice on how to support vulnerable customers in branch.

Customer facing individuals and their managers

We do not expect these people to be able to diagnose vulnerabilities. But we would expect these individuals to, listen to our customers, empathise and ask how we can help meet their needs, preparing to be flexible in meeting their needs where this is possible. In certain, circumstances (Telco call centres) we do also ask that where appropriate they suggest the customer informs us of their vulnerability so we can discuss how we can best meet their needs.

Those involved in the design of products and services and the processes that support their distribution and sale.

Design and processes for customer related projects and processes should consider how a vulnerable customer could take that journey. Gating requirements for customer facing projects should consider customer vulnerability requirements as part of the assessment process.

The Compliance team will provide guidance regarding the legal requirements, regulatory guidance and relevant industry body recommendations, as well as Post Office recommended best practice.

Publication of a telecoms vulnerable customer policy

POL00401629

In accordance with Ofcom's General Conditions regulation, Post Office have a specific telecoms vulnerability policy which is published on our website and reviewed annually. Customer who are vulnerable have vulnerability flags on the system and the call centre is trained accordingly.

1.8 Risk

By not addressing the needs of vulnerable customers, the impact could be significant for those customers that depend on us to deliver our products and services. These risks are included in the minimum control standards section below but could include customers not being able to access our branches, products or services, inappropriate purchases and not being able to understand the features or terms and conditions of a product or service.

It could also cause reputational damage undermining Post Office's achievement of its social purpose. The Department of Business Energy and Industrial Strategy has the protection of vulnerable customers as a key strategic priority for government. Under both Ofcom and FCA rules there could be regulatory interventions for not treating vulnerable customers fairly or having the correct policies in place.

1.9 Legislation

- Ofcom duties under the Communications Act (including the General Conditions of Entitlement)
- Equality Act 2010
- Mental Capacity Act 2005 and guidance
- The Lasting Powers of Attorney, Enduring Powers of Attorney and Public Guardian Regulations 2007
- Disability Discrimination Act (Northern Ireland) 2005.
- Adults with Incapacity (Scotland) Act 2000.
- Consumer vulnerability regulation detailed within the FCA Handbook for CONC and Mortgage Conduct of Business (MCOB).
- FCA General Guidance Consultation July 2020

1.10 Industry Guidance

- FCA website including 2020 consumer research
- UK Finance
- Age UK advice line
- Money Advice Service
- Pensions Advisory Service
- Alzheimer's Society guidance on Mental Capacity Act provisions
- Gov.uk
- Citizen's Advice Bureau

POL00401629

- Ofcom's Fairness Principles
- Ofcom guidelines on Vulnerability

POL00401629

2 Risk Appetite and Minimum Control Standards

2.1 Risk Appetite

A Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

Post Office's risk appetite is **averse** for:

- non-compliance with law and regulations or deviation from its business conduct standards, and
- for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sits outside the agreed Risk Appetite. In exceptional circumstances a Risk Exemption waiver may be granted.

2.2 Policy Framework

Post Office's Board has overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of vulnerable customer matters by reports from its committees including its Audit and Risk Committee.

It is the responsibility of the policy owners to review this policy at least once a year and on an ad hoc basis as necessary to ensure the policy remains effective and up to date.

This policy will be reviewed by The Post Office Risk and Compliance Committee at least once each year from the last date this policy was determined effective.

2.3 Who must comply?

Compliance with this policy is mandatory for all Post Office employees. We will work with our Agency network, Principals and key commercial partners to ensure that where we can the spirit of our approach to vulnerable customers is applied.

2.4 Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks within the defined Risk Appetite statements contained within the table below. To comply with this, mechanisms must be in place within each

POL00401629

business unit or product to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The minimum control standard for the vulnerable customer policy is 'directive' and will be communicated to staff through staff communications and intranet.

POL00401629

The table below sets out some of the key relationships between identified risk, the considered Risk Appetite, and the required minimum control standards:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible
Physical access to the branch network is difficult	**A) Restricted Mobility** A customer may be particularly vulnerable because they have mobility restrictions; this means that it might be difficult for them to gain physical access to our premises. Or to use our facilities in branch (eg Pin Pads)	• Articulated in Accessibility Guidance. We will follow the requirements of the Equality Act and seek where it is possible to do so to make 'reasonable adjustments' to our business premises to allow customers with mobility restrictions to access our business premises. • Where we are not able to make such adjustments we will seek, where it is reasonable to do so, to provide the customer with an equivalent service through other means. For example a Banking process currently exists for DDA/vulnerable customers when they are unable to use the chip & Pin functionality.	Head of Health and Safety
Customer engagement with products and services is not possible or limited because of a vulnerability	**B) Communications Needs** A customer may be particularly vulnerable because they have a hearing or sight impairment, which means they require specially adapted methods of communication.	• We will look to make 'reasonable adjustments' to the way in which we are able to communicate with our customers. For instance for sight impairment, we will seek to ensure that our customer documentation is available in a range of formats to help them understand our product material and product-life cycle communications. • We will meet the accessibility requirements for Public Sector websites and Apps • For hearing impairment, we will seek to provide functioning hearing loops for	All product teams Director Retail Network Digital Team DMB Engineering team

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

		DMB and provide guidance on where to maintain service loops to the wider Network.	
	C) Low Basic Skills A customer may be particularly vulnerable because they have a low level of basic skills and therefore require additional or specialised assistance to effectively make use of our products and services or, during the course of the product life-cycle, interact with us and manage their financial position effectively.	• We will seek to work positively and constructively with customers that have, or appear to have, a low level of basic skills. • We will seek to ensure that the use of jargon is minimised within our documentation. Where it is used we aim to ensure that there is an easy to understand explanation of the term. • We will look to provide sign-posting to free independent sources of information and support that the customer can access in relevant documentation and sections of our websites. • We will seek to explore how to simplify the information that we provide to customers, for example, through the standardised terms and conditions to highlight parts that matter. If appropriate we will engage with government and industry initiatives	All product teams Director Retail Network
	D) Low Financial Capability A customer may be particularly vulnerable because they have a low level of financial capability (e.g. a specific lack of the maths skills and knowledge of financial products or matters) and therefore may require more straight-forward explanations.	• We aim to be clear and fair and not misleading in communications with customers, and wherever possible we will seek to avoid 'jargon'. We will strive to explain our products and services, including associated risks to customers, in a manner which is easily understandable. • We will seek to take reasonable steps to ensure there is sufficient 'sign-posting'	All product teams Director Retail Network

POL00401629

		across our product and service proposition to charities and other not-for-profit organisations that provide independent advice and guidance on financial issues	
	E) Mental Capacity A customer may be particularly vulnerable because they have a mental capacity limitation (for instanced dementia, a learning disability, a development disorder, a neurological disability) that may restrict their ability to appropriately engage with us or make an informed and responsible borrowing decision.	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • We aim in our dealings with a customer who we know, or reasonably suspect has a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will seek to provide all the information required to enable a customer to do this. Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	All product teams Director Retail Network
	F) Age Related Vulnerability A customer may be particularly vulnerable as a consequence of the effects aging can have on an individual; this includes potential memory loss, dementia or the potential for the customer to be 'overwhelmed' by a particular situation.	• Be aware of the Power of Attorney requirements where applicable (refer to Horizon Help) • Post Office should not automatically assume that a customer is vulnerable by virtue of their age. We seek to provide appropriate products and services to customers of different ages. However, it is appropriate in some circumstances to explain clearly risks which relate to ageing customers e.g., for end of life planning products. • We aim in our dealings with a customer who we know, or reasonably suspect has	All product teams Director Retail Network

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

		a mental capacity limitation, to act sympathetically and positively. • We seek to allow a customer sufficient time to weigh-up the information and explanations we have provided and defer a decision to a later date. We will provide all the information required to enable this. • Where possible we should ask if the individual would like to consider this decision with a family member or trusted person.	
	G) Life Event Vulnerability A customer that has or is experiencing a specific adverse 'life event' (for example, redundancy, a bereavement, critical or terminal illness, or a marriage breakdown) could be particularly susceptible to making poor judgements. (Although these triggers may not always have a negative impact on the individual)	• We should aim to treat these customers fairly and with a level of sympathy and positivity. We aim to ensure, throughout our businesses, that when we become aware of these life events we have the ability to respond flexibly and deliver an outcome that is appropriate.	All product teams Director Retail Network
	H) Financial Difficulties Customers that are in financial difficulties (for instance high levels of debt or low levels of income) may be particularly vulnerable to financial detriment.	• Be conscious of customers in financial difficulties when designing or introducing products and services that require a regular financial commitment • Be able to manage expectations e.g., declines or alternate payment methods if applying for a product or service • Where feasible signpost Money Advice Service, Citizen's Advice Bureau, Pensions Advisory Service and/or other similar independent advice/helplines	All product teams Director Retail Network

POL00401629

3 Where to go for help

3.1 Additional Policies

This policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.2 How to raise a concern

Any Post Office employee who is concerned about the application of this policy should:

- Discuss the matter fully with their Line Manager; or,
- Report their concerns to the policy owner.
  If you wish to do this anonymously you should contact the 'Speak Up' line on GRO.

3.3 Who to contact for more information

If you need further information about this policy, please contact Paul Beaumont.

3.4 Company Details

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

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

Version Control

Date	Version	Updated by	Change Details
July 2017	Draft 0.1	Jonathan Hill / Paul Beaumont	1st draft in revised template
11th July 2017	Draft 0.2.1	Jonathan Hill / Paul Beaumont	2nd draft in revised template
26 Sep 2017	Final 1.0	Paul Beaumont	Approved by ARC on 25/9/2017
30 October 2018	Update 1.1	Paul Beaumont	Annual refresh approved by ARC on 30.10.2018
3 Sep 2019	Update 2.1	Paul Beaumont	Annual refresh await approval from ARC.
23 Sep 2019	3.0	Paul Beaumont	Approved by RCC 03/09/19 Approved by ARC 23/09/19

POL00401629

10 Sep 2020 22 Sep 2020	3.1	Paul Beaumont	Annual refresh RCC review ARC review

POL00401629

1. **Physical Security Policy/Suite**

Policy GE Sponsor	Policy Owner	Contact details	Review history
Mark Raymond	Mark Dinsdale	GRO	September 2019

1.1 Purpose and Content of the Policy

The Policy has been established to set the minimum operating standards relating to the management of our physical security risks throughout the group. The core principles covered by the policy are to aid in ensuring:

- the protection of personnel, Post Office assets and data from physical circumstances and events that could harm our people or cause serious losses or damage.
- protection from crime and terrorism
- the physical security vision and framework

Risks relating to Physical Security can be grouped into the following areas:

- ID Cards
- CCTV
- Lone workers
- Tiger Kidnap or Hostage situations
- Theft or other crime incidents
- Overseas travel

The Policy has been designed to assist in managing the physical security risks to protect our people, branches, buildings and company assets. The overall risk includes the failure to:

- Identify and report risks and threat to the safety of colleagues (during the course of business activities), customers, branches, buildings and assets.
- Gather and assess security threat monitoring intelligence.
- Properly conduct and refresh Business Unit Risk Assessments (including risks assessments in the branch network) to highlight key activities.
- Assess the risk ratings of group buildings and undertake building risk assessments in line with the agreed schedule and standards.
- Assess the impact of changes to new / existing buildings including refurbishments.
- Implement findings of branch, Business Unit and building risks assessments in line with risk appetite
- Act / communicate upon security threat monitoring intelligence.
- Provide the adequate level of surveillance and monitoring over group buildings.
- Prevent unauthorised access to Group sites.
- Deliver required level of colleague protection.
- Respond to an incident and investigate root cause to identify key outcomes and learnings.

It also makes reference to Cognisance being made from a terrorism perspective in light that it currently presents a major threat to businesses. Terrorist groups may seek to cause harm to the economy as a whole by attacking business premises or they may seek to attack specific businesses to advance their political agendas. Whilst there are no

POL00401629

specific threats to Post Office Ltd, considerations should be made of a potential terrorist threat (explosive, hostile vehicle, lone wolf etc).

Through this approach, the Group will maintain customer confidence, protect the Group's customers, colleagues, commercial interests and reputation

1.2Key definition

Physical Security is the protection of people, property and physical assets from actions and events that could cause damage or loss. It describes security measures that are designed to deny unauthorised access to facilities, equipment and resources and to protect personnel and property from harm.

1.3Who Must Comply

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

1.4Key Laws and Regulations

I. Health and Safety at Work Regulations 1999

1.5Risk Appetite and Minimum Control Standards

The Group is exposed to a number of risks and threats relating to Physical Security and the Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group have an Averse risk appetite towards Physical Security.

The policy outlines minimum control standards across 11 areas of risk. Below is an example of the relationships between the risk area and the required minimum control standards to meet the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Operational Security Management	an adversary will attempt to identify and then exploit any perceived weakness within protective security measures	Prevention Control: Adhere to the requirements in the Security Operations Manual which can be found on the intranet and Horizon. Compliance measured via branch training & audits with corrective actions put in place as required.	Postmasters	Ongoing

POL00401629

Physical Security Policy

Version –V2.2

12

POL00401629

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 3
1.5. Legislation 4
1.6. Industry Guidance 4
2. Risk Appetite and Minimum Control Standards 5
2.1. Risk Appetite 5
2.2. Policy Framework 5
2.3. Who must comply? 5
2.4. Minimum Control Standards 6
3. Tools & Definitions 11
3.1. Tools 11
3.2. Definitions 11
4. Where to go for help 13
4.1. Additional Policies 13
4.2. How to raise a concern 13
4.3. Who to contact for more information 13
5. Governance 14
5.1. Governance Responsibilities 14
6. Control 15
6.1. Policy Version 15
6.2. Policy Approval 15
Company Details 16

12

[1]In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.

[2]In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

POL00401629

1. Overview

1.1. Introduction by the Policy Owner

The Network Operations Director has overall accountability to the Board of Directors for the design and implementation of controls for the physical protection of Post Office people and assets, and physical security is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of our physical security risks throughout the group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the group.

This policy sits over a number of Security Sub-Policies including:

- CCTV Deployment Policy and Code of Practice
- Lone Worker Policy
- Tiger Kidnap or Hostage Policy
- Incident Management Policy
- Overseas Travel Policy

Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3. Core Principles

The core principles covered by this policy are to aid in ensuring:

- the protection of personnel, Post Office assets and data from physical circumstances and events that could harm our people or cause serious losses or damage.
- protection from crime and terrorism
- the physical security vision and framework

By implementation of mitigating controls as defined in the minimum control standards of this document, PO can lower the risks against the above threats.

12

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

In exceptional circumstances, where risk sits outside of the Groups's accepted Risk Appetite a Risk Exception can be granted. For further information in relation to the risk exception process please contact the Risk & Assurance team.

For definitions please see section 3.1.

POL00401629

The risk to the Group in relation to physical security is reviewed by the board annually.

1.5. Legislation

All employers have a responsibility, as far as reasonably practicable, to provide a workplace that is safe and secure. In Great Britain, the general duty set out in the Health and Safety at Work Act 1974 to protect the health and safety of employees applies to risks from violence, just as it does to other risks at work

1.6. Industry Guidance

Effective physical security is achieved by multi-layering the different measures. The concept is based on the principle that the security is not significantly reduced with the loss of any single layer. Each layer of security may be comprised of different elements, including for example:

- Measures to assist in the detection of threat weapons, including for example explosives, knives, firearms etc.
- Measures to assist in the detection, tracking and monitoring of intruders and other threats
- Access control and locking systems
- Physical and active barriers to deny or delay the progress of adversaries
- Measures to protect people or assets from the effect of blast or ballistic attack
- Measures to protect sensitive (e.g. classified) material or assets
- Command and control
- The response to an incident
- Security personnel

The above measures are interdependent and their effectiveness will be dictated by their ability to support one another.

Cognisance must also be made from a terrorism perspective in light that it currently presents a major threat to businesses. Terrorist groups may seek to cause harm to the economy as a whole by attacking business premises or they may seek to attack specific businesses to advance their political agendas. Whilst there are no specific threats to Post Office Ltd, consideration when completing this report should be made of a potential terrorist threat (explosive, hostile vehicle, lone wolf etc).

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has:

- Averse appetite to any physical harm to our people or Post Office assets
- Tolerant risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- Averse risk appetite for litigation in relation to high profile cases/issues
- Averse risk appetite for ligation in relation to Financial Services matters
- Averse risk appetite for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the Group
- Averse Risk Appetite in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required.

2.2. Policy Framework

Post Office has established an overarching policy, the Physical Security Policy and a suite of key policies on a risk sensitive approach which are subject to an annual review. Clear policies and procedures support effective decision making and delegation because they provide guidance on what people can and cannot do, what decisions they can make and what activities are appropriate. Having up-to-date and appropriate policies is an important part of our general control environment and supports us in achieving our objectives and protecting our reputation, in an efficient manner.

2.3. Who must comply?

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

Where non-compliance is identified the matter must be referred to the Directors of Risk and Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

POL00401629

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Operational Security Management	An adversary will attempt to identify and then exploit any perceived weakness within protective security measures	Prevention Control: Adhere to the requirements in the Security Operations Manual which can be found on the intranet and Horizon. Compliance measured via branch training, security health checks & audits with corrective actions put in place as required.	Postmasters	Ongoing
CCTV Management	Lack of visible deterrents (such as CCTV) can cause adversary's to attempt crime that the existence of such would otherwise deter. Breach of the Data Protection Act. Lack of adherence to British Standards NSI NACOSS Gold Scheme, NCP 104.3	Prevention Control: All CCTV systems must be deployed in accordance with the CCTV Deployment Policy and operated in accordance with CCTV Code of Practice. Supplier installs to NSI NACOSS Gold Scheme Standards & NSI NCP code of practice for design, installation and maintenance of CCTV surveillance systems 104.3 Standards	CCTV Supplier and Postmasters	At Installation/upgrade or maintenance and every day for operations.
Intruder Alarms	Lack of adherence to British Standards EN 50131-1, NSI NACOSS Gold Scheme, NI ARC Gold Scheme, ISO14001, ISO9001, & ISO 27001	Prevention Control: Creation of specific alarm intruder standard and operating instructions (as detailed in the Security operations Manual). Supplier installs to NSI NACOSS Gold Scheme Standards, NSI ARC Gold Scheme Standards, ISO 14001 design, installation monitoring and maintenance, ISO 9001 & ISO27001	Intruder Alarm Supplier & Postmasters	Ongoing

POL00401629

Access Control	Adversarial individuals could access sensitive, personal or company data.	Prevention Control: Access to branch secure areas will only be given to formally identified and authorised persons, whether Post Office employees, contractors or visitors. Access must be controlled in accordance with the Post Office Security Operations Manual. Access to customer support and supply chain locations must be controlled in accordance with the Post Office ID Cards Policy or Supply Chain Process S 5.2.9: Control of Visitors and Staff, which must include a formal authorisation and identification procedure. Furthermore, a procedure must be deployed to ensure that all staff, contractors and visitors shall always be recognisable by the wearing of a photographic identity card (staff and contractors) or a visitor's badge	Postmasters Customer support and supply chain reception staff	Ongoing Ongoing
Branch Format	Location of a branch can dictate the likelihood of individuals who could act against our staff.	Prevention Control: Post Office operate a suite of branch formats which are defined by several risk factors. Risk assessments are conducted using the Robbery Risk Model or Security function in IMaps, and the format of individual branches is specified by the outcome of this assessment and in accordance with the guidance within the Format Standards documentation. Thereafter, any changes to branch format will only occur following an updated branch risk assessment.	Physical Security – Robbery & Burglary Risk Model	When branch modifications are made
ATM Protection	As these contain cash, adversaries target them to steal the cash using a variety of techniques on a regular basis.	Prevention Control: The Bank of Ireland has installed ATMs at many branches across the Post Office estate; some of these ATMs are serviced directly by Supply Chain, whilst others are serviced by	Postmasters	Ongoing

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

		branches themselves following delivery of cash by Supply Chain. To assure the physical security of each ATM across the Post Office estate, branches must adhere to the security instructions within the Post Office Security Operations Manual. Compliance measured via branch training & audits with corrective actions put in place as required.		
Safe Management	As these contain cash (and other sensitive assets), adversaries target them to steal the cash using a variety of techniques on a regular basis.	Prevention Control: Regardless of safe type it is incumbent on postmasters to ensure that the safe(s) installed operate correctly and that they are used for their designated purpose. To assure the physical security of each safe, branches must adhere to the security instructions within the Post Office Security Operations Manual. Compliance measured via branch training & audits with corrective actions put in place as required.	Postmasters	Ongoing
Bank of England Note Circulation Scheme	Loss of approval to move cash and notes.	Prevention Control: Post Office Supply Chain are members of the Bank of England Note Circulation Scheme and must comply with the security standards of the Scheme at all times in order to retain membership. These standards include specific physical security measures which must be in place and these standards are audited by the Bank on an annual basis. Supply Chain have a robust set of security processes that are operated across Supply Chain premises and vehicles to assure compliance with those standards. Risk assessments are carried out to review the threat of a criminal attack directed against Supply Chain premises and vehicles and	Supply chain managers Security Managers	Ongoing Ad-hoc

POL00401629

		assess the impact on employees who may in the course of their work be exposed to injury from such incidents. Security control measures are constantly reviewed to reduce the risk of criminal attack, with physical security taking into account the intelligence to minimise the likelihood of robbery and resulting injury against either the employees or loss of assets		
Burglary & Robbery		Prevention Control: The Physical Security team own the robbery/ burglary risk model which is based on various key influencing factors to support the Physical Security strategy. The model supports branch formats, identifying branches at risk of further incidents, helping to target robbery and burglary prevention activities so that fewer incidents occur and identify the parameters affecting risk and the likely impact that implementing mitigation will have on risk. The model is reviewed on an annual basis to ensure it includes changes to the underpinning influencing factors.	Security Team	Ongoing, Annually updated
Compliance Checks	All of the above risks	Prevention Control: Announced and Unannounced visits to random branches to test the integrity of and compliance with branch security procedures (Security Health Checks) Test the integrity of and compliance with Supply Chain security procedures (cross pavement observations, operation stripe, premise attack plans)	Security Managers Security Managers Physical Security	Ad Hoc Ad hoc Annually

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

		Review of customer support centres to assess vulnerabilities/ risks and make recommendations for additional physical security measures to mitigate those risks. When a robbery/burglary incident occurs at branches, post-incident reviews are carried out to investigate the incident thoroughly working in conjunction with law enforcement agencies. If physical security risks are identified during the review, recommendations for additional security measures are made to mitigate those risks. Security management information reports are issued on a regular basis to the Physical Security Forum for oversight and review.	Security Managers	Ad Hoc
Governance	All the above Risks	Prevention Control: Assess compliance with the Physical Security family of policies. Regular supplier service reviews are completed to ensure governance with supplier contracts and to address any service issues identified.	The Security Governance Forum. Supplier Management Team	Ad hoc Monthly/ quarterly

POL00401629

3. Tools & Definitions

3.1. Tools

Robbery & Burglary Risk Model

ATM Risk Model

CViT Risk Model

3.2. Definitions

CViT	Cash and Valuables in Transit
Supply Chain	Cash centres/depots and vehicles
Post Office Group ("Post Office")	Post Office Limited and all subsidiaries and entities within the Post Office Group which includes Post Office Management Services and FRES
Policy Owner	As defined by the Post Office Policy Framework-Roles and responsibilities Matrix document
Security Operations Manual	A set of procedures and instructions for postmasters to follow in the operational security management of their branch
CCTV Deployment Policy	Defines the framework for CCTV deployment throughout Post Office estate, CViT fleet and customer support centres
CCTV Code of Practice	Details requirements by Post Office for the operation of CCTV systems in it premises to ensure compliance with the Data Protection Act 1998
Data Protection Act 1998	This Act sets out legal requirements for compliance where personal data is captured and processed
ID Cards Policy	Sets out policy for access control for staff and visitors at Post Office cash and stock centres, cash depots and customer support centres
Bank of England Security Standards of the Note Circulation Scheme	These standards are the minimum standards set and updated by the Bank of England from time to time that must be met by cash

POL00401629

	centres who are part of the Note Circulation Scheme
S5.2.9 Control of Visitors and Staff – Supply Chain Operational Unit	Procedures for access control at Supply Chain centres and depots
PCI Data Security Standard	Standards/controls established by the PCI Security Standards Council to maximize security of cardholder data
Formats Standard	A set of standards documents that define security requirements for different branch formats
Security Governance Forum	The Security Governance Forum provides governance and decision making for all security matters, both policy-wise and operational

POL00401629

4. Where to go for help

4.1. Additional Policies

This Policy is one of a set of sub-policies set out below, this being the overarching policy:

- CCTV Deployment Policy and Code of Practice
- Lone Worker Policy
- Tiger Kidnap or Hostage Policy
- Incident Management Policy
- Overseas Travel Policy

The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach of this Policy should report this without any undue delay. Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: GRO or by telephone on: GRO.
- The confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO, or
- Via a secure on-line web portal: http://postoffice.ethicspoint.com/

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Correspondence Team.

12

4.3. Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact the Policy sponsor or Policy Owner.

POL00401629

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the Network & Sales Director of Post Office Limited.

The Policy owner is the Head of Loss Prevention who is responsible for ensuring that the Physical Security Team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Head of Loss Prevention is responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

POL00401629

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
Draft v1.0	08/04/2016	Diana Maddox	First draft for new policy framework
Draftv1.1	13/04/16	Mark Rodgers	Policy Standards review
Draft 1.2	21/04/16	Diana Maddox	Amendments following Policy Standards review
Ver 1.3	23/11/16	Mark Dinsdale	Annual Review, update policy owner etc.
Ver 1.4	20/11/17	Mark Dinsdale	Annual Review
Ver Draft 1.5	12/06/2018	Mark Dinsdale	Conversion to new policy template and minor updates for GDPR.
Ver 1.6	17/01/2019	Mark Dinsdale	Amendments following GDPR review
Ver 2.0	27/09/2019	Mark Dinsdale	Approved by RCC & ARC
Ver 2.1	09/07/2020	Mark Dinsdale	Annual Review
Ver 2.2	27/08/2020	Mark Dinsdale	Updated Whistleblower details & Annual Review

6.2. Policy Approval

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

Committee	Date Approved
POL R&CC	27 September 2019
POMS R&CC	27 September 2019
POL ARC	27 September 2019
POMS ARC	27 September 2019

12

Policy Sponsor: Network Operations Director

Policy Owner: Head of Security, Safety & Loss Prevention

Policy Author: Senior Security Manager

Next review: 1 Aug 2021

POL00401629

Company Details

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

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

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

POL00401629

1. HMRC Fit and Proper Standards Policy

Policy GE Sponsor	Policy Owner	Contact details	Review history
Ben Foat	Sally Smith	GRO	September 2020

1.1 Purpose and Content of the Policy Standard

Sets the minimum operating standards relating to the design and implementation of controls to ensure that the Fit & Proper Requirements under the Money Laundering Regulations 2017 (MLRs) are complied with throughout the Group. It is sub-ordinate to the Anti-Money Laundering and Counter Terrorist Financing Policy (AML/CTF) which provides a clear risk and governance framework and an effective system of internal control for the mitigation of risk across the Group.

Post Office is supervised by HM Revenue and Customs (HMRC) for anti-money laundering purposes in relation to its Money Service Business (currently Branch on-demand and pre-order Bureau de Change) and is therefore subject to the regulatory fit and proper requirements.

The requirements are designed to ensure that those individuals and agents that are responsible for overseeing relevant activity are suitable to undertake those roles. Post Office has devised a robust policy standard and associated procedures which are proportionate to the risks and complexity of the Group.

The governance arrangements described in the policy standard are based on the following taking place:

- The Group ensures that its policies reflect the principles of the AML and CTF regulations and legislation;
- The Group's overall and ongoing risk management process includes a risk based assessment of the risks to which the Group and its business are exposed, and the quality of its AML and CTF controls and monitoring;
- The Group undertakes a training and awareness program to ensure employees and agents are aware of the risks of money laundering and terrorist financing, what they should do if they are suspicious, and the consequences should they fail to comply with the law;
- The Group promotes ethical and professional standards to prevent it from being used, intentionally or unintentionally by criminals;
- Decisions taken by management are consistent with the Board's approved strategic objectives and Risk Appetite;
- Every member of staff is responsible for understanding and managing the risks they take on behalf of the Group;
- Clear accountabilities are delegated by management to staff who have the right level of skill, competency and experience;
- All employees are required to comply with Group Policies.

1.2 Key definition

Money laundering is the process whereby criminals retain, disguise and conceal the proceeds of their crimes, or raise, consolidate or retain funds for use in **financing terrorism**. In UK law money laundering is defined in the Proceeds of Crimes Act 2002 (POCA) and includes all forms of handling or possessing criminal property, including possessing the proceeds of one's own crime, and facilitating any handling or possession of criminal property.

Failure to manage AML/CTF risks can result in financial loss, customer impact, terrorism, regulatory breaches, fines, prosecution, prevention from selling a particular product, loss of existing or future contracts/relationships and damage to reputation.

HMRC Fit and Proper – HMRC requires that all those designated as responsible persons in businesses regulated by them under the MLRs apply for and undertake the HMRC Fit & Proper test, or that they have (and can demonstrate that they have) controls in place to ensure the responsible persons of their agents are fit and proper.

POL00401629

1.3 Who Must Comply

All Post Office employees, agents and Commercial Partners and applies wherever in the world the Group's business is undertaken.

1.4 Key Laws and Regulations

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("Money Laundering Regulations") apply to the Post Office as an MSB registered with HMRC, and along with HMRC guidance, sets out the requirements for Fit & Proper tests to include all relevant senior managers, agents and beneficial owners.

1.5 Risk Appetite and Minimum Control Standards

The policy standard defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite. It also outlines the Post Office's definition of responsible persons and incorporates a list of impacted Direct Employee roles.

Post Office has an Averse risk appetite for financial crime to occur within any part of the organization. Non-compliance with the Policy Standard could result in suspension or cancellation by HMRC of Post Office's MSB registration, prohibition of an individual from holding a managerial role, reputational damage, court orders and regulatory inspections, prosecution of individuals within Post Office and financial penalties, which are publicly notified.

The policy outlines minimum control standards across 7 areas of risk. Below is an example of the relationships between the risk area and the required minimum control standards to meet the stated risk appetite:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Direct Employees	Failure to identify all roles within Post Office that are engaged with overseeing regulated activity	Directive control: The GE and the Group Chief People Officer are responsible for approving the list of impacted 'responsible person' roles.	GE and Group Chief People Officer	Annually
		Preventative Control: The list of impacted roles is maintained in success factors and subject to regular review to ensure that all roles that provide oversight of MSB regulated activity (including project managers, sales managers and those responsible for overseeing agent on-boarding, training and contractual activity) or that may otherwise fall into the 'responsible persons' category have been identified.	Group Chief People Officer & MLRO	Annually
		All job profiles for impacted roles must include the requirement for the individual to pass the HMRC Fit & Proper test in order to undertake the role.	Group Chief People Officer	Ongoing

12

POL00401629

POST OFFICE

POLICY STANDARD

HMRC Fit and Proper Policy Standard: Employees, Agents and Commercial Partners

Version – V2.1

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This policy supports these to help us ensure that wherever possible use of Post Office systems and products for money laundering or terrorist financing is prevented, and the highest standards of financial crime prevention, detection and management are maintained.

POL00401629

Table of Contents

1. Overview 34
1.1. Introduction by the Standard Owner 34
1.2. Purpose 34
1.3. Core Principles 34
1.4. Application 45
1.5. Legislation 56
1.6. Consequences of Post Office not complying with the Fit and Proper requirements 56
2. Risk Appetite and Minimum Control Standards 78
2.1. Risk Appetite 78
2.2. Standard Framework 78
2.3. Who must comply? 78
3. Where to go for help 1516
3.1. Additional Policies 1516
The full set of policies can be found at: 1516
https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx 1516
3.2. How to raise a concern 1516
3.3. Who to contact for more information 16
4. Governance 17
4.1. Governance Responsibilities 17
5. Document Control 18
5.1. Document Control Record 18
Company Details 18

12

POL00401629

1. Overview

1.1. Introduction by the Standard Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent and deter Financial Crime, which includes Anti Money Laundering (AML) and Counter Terrorist Financing (CTF). Compliance~~Financial Crime~~ is an agenda item for the Audit and Risk Committee and the Post Office Board is updated as required.

1.2. Purpose

This policy standard has been established to set the minimum operating standards relating to the design and implementation of controls to ensure that the Fit & Proper Requirements under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 are complied with throughout the Group. It is sub-ordinant to the Anti-Money Laundering and Counter Terrorist Financing Policy which provides a clear risk and governance framework and an effective system of internal control for the mitigation of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3. Core Principles

Money Laundering and Terrorist Finanacing are criminal offences and everyone working in the business has a personal obligation to prevent them taking place. Post Office is supervised by HM Revenue and Customs (HMRC) for anti-money laundering purposes in relation to its Money Service Business (MSB) (currently Branch on-demand and pre-order Bureau de Change) and is therefore subject to the regulatory fit and proper requirements. These requirements are designed to ensure that those individuals and agents that are responsible for overseeing relevant activity within the regulated parts of the business are suitable people to undertake those roles.

Post Office[1] has devised a robust policy standard and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group. The governance arrangements described in this policy standard are based on the following taking place:

- The Group ensures that its policies reflect the principles of the AML and CTF regulations and legislation;

- The Group's overall and ongoing risk management process includes a risk based assessment of the risks to which the Group and its business are exposed, and the quality of its AML and CTF controls and monitoring;

[1] [1] In this Standard "Post Office" means Post Office Limited.

POL00401629

• The Group undertakes a training and awareness program to ensure employees and agents are aware of the risks of money laundering and terrorist financing, what they should do if they are suspicious, and the consequences should they fail to comply with the law;

• The Group promotes ethical and professional standards to prevent it from being used, intentionally or unintentionally by criminals;

• Decisions taken by management are consistent with the Board's approved strategic objectives and Risk Appetite;

• Every member of staff is responsible for understanding and managing the risks they take on behalf of the Group;

• Clear accountabilities are delegated by management to staff who have the right level of skill, competency and experience;

• All employees are required to comply with Group Policies.

1.4. Application

This policy standard is applicable to Post Office Ltd Money Service Business (MSB) and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

• Post Office Ltd's "Responsible Persons" are defined as:

- Officers of the business, including directors and the company secretary, and any other person who effectively directs the business, for example members of any board that makes decisions about the direction of the business or financial decisions, is a signatory to its bank account, has significant staff management responsibilities or has power to appoint and dismiss employees.
- Senior managers who are engaged directly in the provision of the relevant MSB activity. This includes managers who influence or make decisions affecting compliance (this includes product managers and senior managers overseeing sales activity in the branch network), and individuals Post Office employs to oversee or manage the screening, ~~and~~ propriety and training of our agents, but not managers who are not routinely involved in the AML and CTF policies and procedure of the business.
- The nominated officer for the purpose of reporting of suspicions of money laundering and terrorist financing (MLRO).
- The beneficial owners, Agents and Commercial Partners[2] that operate a Post Office and (where the agent it not an invididual) their partners, limited company directors, secretaries and beneficial owners.

See Appendix A for a list of impacted Direct Employee roles

• Compliance with the Fit and Proper Requirements includes (but is not limited to):

Commented [SS1]: Amended to include teams responsible for training of agents as this is a key MLR requirement

12

[2] A 'Commercial Partner' is a multiple retailer or strategic alliance with an established relationship with POL. These partners have a strong balance sheet (working capital and bank balance), and will usually have a national presence or significant regional presence, and typically centralised functions including Head Office support……..

POL00401629

- Ensuring Post Office Directors, Company Secretary, General Executives (GE), beneficial owners and designated employees who are Responsible Persons have passed the HMRC Fit and Proper Test and have received sufficient training to undertake their roles
- Assessing our agents directly or requiring our commercial partners to assess that, within their organisation, any Responsible Person:
  - does not have any unspent convictions for offences set out in Schedule 3 to the Money Laundering Regulations;
  - has disclosed to us certain other criminal convictions or regulatory, supervisory or disciplinary actions that may be relevant to an assessment of honesty and integrity;
  - has the requisite competence and capabilities (including any necessary training) *See Appendix B for Training Matrix;*
  - remains financially sound (including tax affairs).

The criteria for the assessment of financial soundness for fit & proper purposes is set out in the Fit & Proper Team's processes. These processes are subject to annual review and approval by the Declarations Oversight Committee.

Commented [SS2]: Amended to reflect practice

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risk of Post Office being used to facilitate Money Laundering or Terrorist Financing activities, and therefore takes a risk based approach.

Failure to comply with the requirements of this policy standard by any employee will be regarded as a significant breach impacting on the Group's risk and control environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

Where an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence (for direct employees) or as a contractual breach (for agents).

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. Further information in relation to the risk exception process, together with a template can be found on the Intranet *(link)*

The risk to the Group in relation to Money Laundering and Terrorist Financing is reviewed by the Board as part of its wider commitment to Financial Crime on a regular basis.

1.5. Legislation

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("Money Laundering Regulations") apply to the Post Office as a MSB registered with HMRC, and set out the requirements for Fit & Proper tests to include all relevant senior managers, agents and beneficial owners.

1.6. Consequences of Post Office not complying with the Fit and Proper requirements

If Post Office does not comply with the fit and proper requirements it could be subject to:

POL00401629

- Suspension or cancellation by HMRC of Post Office's MSB registration, resulting in the suspension or withdrawal of our Bureau de Change product, and subsequent damage to Post Office Brand and/or loss of other business (e.g. acting as an agent for MoneyGram)
- Prohibition of an individual from holding a managerial role
- A public statement naming and censuring the business or a person, which can cause serious branch impact and reputational damage
- Court orders and regulatory inspections
- Prosecution of individuals within Post Office
- Financial penalties, which are publically notified

POL00401629

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day business transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has:

- **Tolerant risk** appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk** appetite for litigation in relation to high profile cases/issues
- **Averse risk** appetite for litigation in relation to Financial Services matters
- **Averse risk** appetite for not complying with law and regulations or for deviation from business' conduct standards for financial crime prevention within any part of the Group
- **Averse Risk** Appetite in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required.

2.2. Standard Framework

Post Office has established a suite of financial crime prevention policies and procedures, on a risk sensitive approach, which are subject to annual review. The policy suite is designed to combat money laundering, terrorist financing, bribery and corruption, facilitation of tax evasion, fraud and ensure adherence to relevant sanctions regimes.

The HMRC Fit & Proper Policy is a policy standard relating to the Anti-Money Laundering and Counter Terrorist Policy and should be considered and read in conjunction with the overarching Financial Crime Policy where relevant.

2.3. Who must comply?

Compliance with this policy standard is mandatory for all Post Office employees[3], agents and Commercial Partners and applies wherever in the world the Group's business is undertaken.

Commented [SS3]: Definition updated to reflect currently approved definition in AML.CTF policy

12

3 In this policy "employee" and "staff" means all persons working for the Group or on our behalf in any capacity including employees at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, and contractors.~~In this Standard "employee" means permanent staff, contractors, consultants and anyone else working for or on behalf of Post Office.~~

POL00401629

Where non-compliance is identified the matter must be referred to the MLRO and the Group ~~HR Director~~Chief People Officer. Any investigations will be carried out in accordance with the Investigations Policy. Where an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence (for direct employees) or as a contractual breach (for agents and Commercial Partners).

Commented [SS4]: Amended title

POL00401629

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Direct Employees	Failure to identify all roles within Post Office that are engaged with overseeing regulated activity	Directive control: The GE ~~and HMRC Fit & Proper Declaration Oversight Committee (DOC)~~and the Group Chief People Officer are responsible for approving the list of impacted 'responsible person' roles.	GE and Group Chief People Officer	Annually
		Preventative Control: The list of impacted roles is maintained ~~by HR~~in Success Factors and subject to regular review to ensure that all roles that provide oversight of MSB regulated activity (including project managers, sales managers and those responsible for overseeing agent on-boarding, training and contractual activity) or that may otherwise fall into the 'responsible persons' category have been identified.	Group ~~Human Resources Director~~~~Cheif~~ Chief People Officer & MLRO	Annually
		All job profiles for impacted roles must include the requirement for the individual to pass the HMRC Fit & Proper test in order to undertake the role.	Group ~~Human Resources Director~~Chief People Officer	Ongoing

Formatted: Left

Formatted: Left

Commented [SS7]: Amended title

Commented [SS5]: Amended as the focus of the DOC is purely agents, not direct employees

Commented [SS6]: Amended as SF now includes a mandatory field to show whether a role is subject to HMRC F&P

Commented [SS8]: Amended title

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Direct Employees	Failure to ensure 'responsible persons' are adequately vetted and pass the HMRC Fit & Proper Test	Preventative control: All Board members, GE, the MLRO and designated responsible persons must undergo pre-employment screening and vetting as outlined in the Post Office Group Staff Vetting Requirements Policy and pass the HMRC Fit and Proper Test before being appointed. ~~For those employees that transfer into a responsible persons role within Post Office will undertake a DBS, Credit and Voters Roll, PEPS and Sanction check as well as the HMRC Fit and Proper Test.~~ Where an exisiting employee fails Post Office screening or the HMRC Fit & Proper Test Post Office will consider redeployment or dismissal in accordance with HR policies. Detective control: Post Office Group may require vetting to be rechecked or verified at any time during the employment term as determined by service contractual obligations, regulatory requirements, internal and external audit purposes, periodical re-certification or at Post Office Group's discretion.	Group ~~Human Resources Director~~Chief People Officer ~~Group Human Resources Director~~ Group ~~Human Resources Director~~Chief People Officer Group ~~Human Resources Director~~Chief People Officer	Ongoing Ongoing Ongoing Ongoing

Formatted: Left

Formatted: Left

Commented [SS10]: Amended title

Commented [SS9]: Deleted as assessed this is not required as all individuals are vetted upon employment and HMRC undertake some checks as part of the F&P process

Commented [SS11]: Amended title

Commented [SS12]: Amended title

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Direct Employees	Failure to keep Fit & Proper tests and records up to date	Directive control: All impacted 'responsible persons' are required to notify their line manger or HR immediately if they believe that they no longer meet the requirements of the fit and proper test. All records relating to on-boarding screening and vetting and the outcome of HMRC fit & proper tests must be maintained for the duration of that individual's employment and made available to HMRC for inspection, if required. ~~Preventative control:~~ ~~All impacted 'responsible persons' are required to complete an annual declaration that they meet the requirements of the fit and proper test. Failure to do so will lead to a review by HR and line management to establish if the individual is able to continue to undertake aspects of their role.~~	Roles as listed in Appendix A Group ~~Human Resources Director~~Chief People Officer and MLRO ~~Group Human Resources Director~~	Ongoing Annually ~~Annually~~
Direct Employees	Failure to provide adequate training in relation to regulated activity	Preventative control: Post Office has on-boarding and on-going training programmes to ensure that all employees, including 'responsible persons' receive adequate training to undertake their role Post Office requires all employees to complete mandatory AML/CTF training within 30 days of joining and annually	Line Managers, The People Function and ~~HR~~ Learning & Development ~~MLRO and Group Human Resources Director~~The People Function	Ongoing Annually

Formatted: Left

Formatted: Left

Commented [SS13]: Deleted, as assessed that performance management and current HR policies and Code of Business Standards are sufficient

Formatted: Left

Commented [SS14]: Amended title

Commented [SS15]: Amended to reflect AML/CTF policy and function title change

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Agents & Commercial Partners	Failure to ensure those individuals applying to operate Post Offices that are 'responsible persons' are 'fit and proper' to undertake Post Office regulated activity	Preventative control: Prior to contract approval, all agents and 'responsible persons' (partners, directors, company secretaries, beneficial owners (holding a stake of 25% or more) and ultimate beneficial owners) must undergo screening and vetting, including evidencing that they have no Schedule 3 convictions, as outlined in the Postmaster Vetting Requirements Policy.	~~Group Human Resources Director and Retail Operations Director~~ Onboarding team	Ongoing
		Post Office has on-boarding and on-going training programmes to ensure that all agents, including 'responsible persons' receive adequate training to undertake their role.	Postmaster Training, Design & Delivery ~~Retail Operations Director and HR Learning & Development~~	Ongoing
		Post Office requires all counter staff to complete mandatory AML/CTF training before they transact on Horizon and annually.	~~MLRO & Group Human Resources Director~~Learning & Development	Ongoing

Formatted: Left

Formatted: Left

Commented [SS16]: Amended responsibility following business changes

Commented [SS17]: Amended responsibility following business changes

Formatted: Left

Commented [SS18]: Amended responsibility following business changes

POL00401629

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Agents & Commercial Partners	Failure to keep fit and proper tests and records up to date	Directive control: Agents are required to notify Post Office immediately of any changes to 'responsible persons' or their status.	~~On-boarding~~Fit & Proper Team	Ongoing
		Commercial Partners: The Commercial partner is responsible for ensuring that each 'responsible person' in their organisation has undertaken the requisite job-related and compliance training, have the 'Right to Work) and do not hold a Schedule 3 conviction.	~~Group Human Resources Director~~Commercial Partner Relationship Managers	Ongoing
		All records relating to on-boarding screening, vetting and training must be maintained for the duration that the 'responsible person' is party to the contract between the agent and Post Office, and made available to HMRC for inspection, if required.	Onboarding Team & Business Plans Finance Team ~~Group Human Resources Director & MLRO~~	Ongoing
		Where Post Office identifies concerns about an agents ongoing fitness to operate a post office, Post Office will consider the viability of the agency relationship and the immediate removal of their ability to transact money service business.	Contracts Managers & ~~MLRO~~Declaration Oversight Committee	Ongoing
		Post Office is required to provide to HMRC each month to an agreed schedule all required data on agents and responsible persons (including new, amendments and removal of individuals following contract termination or removal of Travel Money and MoneyGram services, if applicable,).	Fit & Proper Team & MLRO ~~Group Human Resources Director~~	~~Annually~~Monthly

Formatted: Left

Formatted: Left

Commented [SS19]: Amended to reflect practice

Commented [SS20]: Amended responsible teams

POL00401629

		Preventative control: All impacted 'responsible persons' are required to complete an annual declaration that they meet the requirements of the fit and proper test. Where an Agent/Responsible Person fails to provide their declaration by the required date or if they are deemed to no longer meet fit and proper requirements, Travel Money and MoneyGram services, if applicable, will be removed.	~~Fit & Proper and On-boarding~~ ~~Retail Operations Director~~Fit & Proper Team and Declarations Oversight Committee ~~Commercial Partner Account Managers and Retail Operations Director~~	Ongoing ~~Ongoing~~
Risk Area	**Description of Risk**	**Minimum Control Standard**	**Who Responsible**	**When**
Agents & Commercial Partners	Failure to action suspension and/or revoke mandates approved by the ~~HMRC F+P~~ Declaration Oversight Committee (DOC)	Preventative Control: All revoke and suspension decisions will be issued to Fujitsu and FRES in approved formats to ensure MSB functionality is removed in locations identified by DOC mandate Quality Assurance (QA) sample of MDM functionality fields associated with suspended/revoked branches checked to ensure DOC manadate has been actioned in a timely and effective manner	~~Contracts Manager~~Fit & Proper Team ~~Contracts Manager~~Fit & Proper Team	On-going On-going

Formatted: Left

POL00401629

3. Where to go for help

3.1. Additional Policies

This policy standard is a sub-policy within the Anti-Money Laundering and Counter Terrorist Financing Policy

The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

3.2. How to raise a concern

Any Post Office employee who suspects dishonest or fraudulent activity and or a breach of this policy has a duty to:

- Discuss the matter fully with their Line Manager; or,
- Report their suspicions by telephoning Grapevine on GRO ; or,
- Report the matter directly to the Money Laundering Reporting Officer (MLRO)
- Staff can contact the Post Office's Whistleblowing Officer, Post Office General Counsel who can be contacted by email at: GRO or by telephone on: GRO
- the confidential Whistleblowing Speak Up service 'Ethicspoint' provided by Navex Global via telephone on GRO
- or via a secure on-line web portal: https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826

~~• Report their suspicions by telephoning Grapevine on GRO~~

~~• If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: GRO or by telephone on: GRO .~~

~~• Alternatively, staff can use the Speak Up Service~~

~~Contact details for the Speak Up line are:~~

~~• GRO~~

~~• https://wrs.expolink.co.uk/postoffice which is a secure on-line web portal~~

Commented [SS21]: Updated Whistleblowing details

Any Post Office agent who suspects dishonest or fraudulent activity and or a breach of this policy has a duty to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

Post Office encourages members of the public or people not employed by us who suspect activity in breach of this policy to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ**.

POL00401629

3.3. Who to contact for more information

If you need further information about this policy standard or wish to report an issue in relation to this policy, please contact *fitandproper* GRO *or financial.crime* GRO.

POL00401629

4. Governance

4.1. Governance Responsibilities

The policy standard sponsor, responsible for overseeing this Standard is the General Counsel of Post Office Limited.

The policy standard owner is the Compliance Director, who is responsible for ensuring that the People & Policy Compliance Manager conducts an annual review of this Policy and tests compliance across the Group. Additionally, the Compliance Director and the MLRO and People & Policy Compliance Manager are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

POL00401629

5. Document Control

5.1. Document Control Record

SUMMARY			
GE Policy Sponsor	Standard Owner	Standard Implementer	Standard Approver
General Counsel	Compliance Director	~~Senior Manager,~~ People & Policy Compliance Manager	R&CC
Version	Document Review Period	Policy – effective date	Policy location
V2.0	Annually	23rd September 2019	Intranet

Commented [SS22]: Amended title

REVISION HISTORY			
Version	Date	Changes	Updated by
1.1	12/08/2019	Draft version created	Andrew Lewis
1.2	22/08/2019	Appendix 1 updated	Andrew Lewis
1.3	23/08/2019	Draft amendments following review by MLRO	Andrew Lewis
2.0	23/09/2019	Approved by POL RCC and ARC	Sally Smith
2.1	14/08/2020	Annual review, amended role titles and training matrix	Sally Smith

DOCUMENT DISTRIBUTION STATUS			
Distribution	Mark x as appropriate	Document Sensitivity	Mark x as appropriate
Internal	X	Non-sensitive	X
External		Sensitive	

QUALITY STATEMENT	
Quality Control	Next Review Date
This document is periodically reviewed, and at least on an Annual basis starting from the last effective date. This standard has been reviewed against the latest Post Office policy standards and legislative requirements.	~~August 2020~~September 2021

12

Company Details

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

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

POL00401629

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

APPENDIX A - Fit & Proper List – Direct Employee Roles

Commented [SS23]: Updated as per current structure and role titles, plus added in Head of Risk & Branch Standards and SmartID Product Owner as this area is now responsible for agent F&P declarations and reporting

ROLE TITLE
CHAIRMAN
NON-EXECUTIVE DIRECTOR
SENIOR INDEPENDENT DIRECTOR
GROUP CHIEF EXECUTIVE OFFICER
GROUP CHIEF FINANCE OFFICER
GROUP GENERAL COUNSEL
GROUP CORPORATE AFFAIRS AND COMMUNICATIONS DIRECTOR
GROUP CHIEF INFORMATION OFFICER
GROUP CHIEF COMMERCIAL OFFICER
GROUP RETAIL AND FRANCHISE NETWORK DIRECTOR
GROUP CHIEF PEOPLE OFFICER
GROUP OPERATIONS AND SUPPLY CHAIN OFFICER
GROUP MARKETING AND BRAND DIRECTOR
GROUP CHIEF STRATEGY AND TRANSFORMATION OFFICER
MANAGING DIRECTOR, IDENTITY
COMPLIANCE DIRECTOR
COMPANY SECRETARY
MLRO & HEAD OF FINANCIAL CRIME
DIRECTOR POST OFFICE MONEY
PRODUCT DIRECTOR: TRAVEL MONEY
OPERATIONS DIRECTOR
HEAD OF SECURITY, SAFETY OF LOSS PREVENTION
SENIOR CONTRACTS AND LOSS PREVENTION MANAGER
CONTRACT INVESTIGATION AND RESOLUTION MANAGER
CONTRACT ADVISOR
HEAD OF RISK & BRANCH STANDARDS
SMART ID PRODUCT OWNER
NETWORK DEVELOPMENT DIRECTOR
HEAD OF NETWORK
HEAD OF DMB NETWORK
HEAD OF COMMERCIAL PARTNERSHIPS
HEAD OF RETAIL OPERATIONS
REGIONAL MANAGER
AREA MANAGER
DMB OPERATIONAL MANAGER
SENIOR PARTNER RELATIONSHIP MANAGER
SENIOR FIELD BUSINESS DEVELOPMENT MANAGER
PARTNER BUSINESS SUPPORT MANAGER
HEAD OF POSTMASTER ON-BOARDING
REGIONAL OPERATIONS BUSINESS SUPPORT MANGER
REGIONAL TRAINING MANAGER
ON-BOARDING & ASSESSMENT MANAGER

POL00401629

APPENDIX B – Training Matrix

Commented [SS24]: Complete re-write with L&D & Postmaster Training, Design & Delivery teams to reflect current structure and training

The formal training and declarations detailed below are supplemented by periodic communications and awareness via all POL communications delivery channels and the NFSP.

Population	Frequency	Allocation	Tracking	Learning Solution Delivery Mechanism	Learning Solution Content responsible Person	Responsible Person Knowledge Declaration	Anti-Money Laundering (AML)	Product/Horizon Training
Direct Employees branch colleagues (DMB)	On boarding	HRSC	L&D	SuccessFactors (branch managers and support teams)	L&D & Postmaster Training, Design & Delivery	N/A	Yes	Know how to conduct transactions on Horizon Product knowledge training
	Ongoing	Branch Manager/SmartID training controls	Branch Standards	Horizon (counter colleagues)	L&D	N/A	Annually	Updated training as required: Know how to conduct transactions on Horizon Product knowledge training
Direct Employees non branch	On boarding	HRSC	HR	SuccessFactors	L&D	N/A	Yes	N/A
	Ongoing	HRSC	HR	SuccessFactors	L&D	N/A	Annually	N/A
Agents (Sole Traders and Partners) inc Temp Agents With Smart ID	On Boarding	Onboarding Team	Postmaster Training, Design & Delivery	Totara and Classroom Training	L&D & Postmaster Training, Design & Delivery	N/A	Yes	Know how to conduct transactions on Horizon Product knowledge training
	Ongoing	L&D	Branch Standards	Horizon	L&D & Postmaster Training, Design & Delivery	N/A	Annually	Updated training as required: Know how to conduct transactions on Horizon Product knowledge training
Agents (Sole Traders and Partners) inc Temp Agents	On boarding	Onboarding Team	Onboarding Team	Declaration	Postmaster Training, Design & Delivery	Yes	Declaration only	N/A

POL00401629

Without Smart ID	Ongoing	Branch Standards	Branch Standards	Annual Declaration	N/A	N/A	Declaration only	N/A
Limited Company Directors & Beneficial Owners of Agent Limited Co. With SmartID	On Boarding	Onboarding	Postmaster Training, Design & Delivery	Horizon	L&D & Postmaster Training, Design & Delivery	N/A	Yes	Know how to conduct transactions on Horizon Product knowledge training
	Ongoing	L&D	Branch Standards	Horizon	L&D & Postmaster Training, Design & Delivery	N/A	Annually	Updated training as required: Know how to conduct transactions on Horizon Product knowledge training
Directors & Beneficial Owners of Agent Limited Co. Without Horizon Log on	On boarding	Onboarding Team	Onboarding Team	Declaration	Postmaster Training, Design & Delivery	Yes	Declaration only	N/A
	Ongoing	Branch Standards	Branch Standards	Annual Declaration	N/A	N/A	Declaration only	N/A
Commercial Partners Without Horizon Log On	On boarding	Commercial Partners Relationship Managers	Retail Ops	Annual Declaration	N/A	Yes	Declaration only	N/A
	Ongoing	Branch Standards	Branch Standards	Annual Declaration	N/A	N/A	Declaration only	N/A

Post Office Limited - Risk and Compliance Committee-10/09/20

POL00401629

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	22 September 2020
Time:	09.00 – 11.30
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Lisa Cherry (Group Chief People Officer): Item 4
Ken McCall (SID)	Daisie Jope (Head of HR Organisation Effectiveness Project Lead): Item 4
Tom Cooper (NED, UKGI)	Maxine Cross (Head of Reward and Pensions): Item 5
Zarin Patel (NED)	Tim Perkins (Head of Security, Safety & Loss Prevention): Item 6
Regular Attendees:	Mark Dixon (Treasurer): Item 7
Tim Parker (Group Chairman, POL)	Andy Bear (Locktons): Item 7
Nick Read (Group CEO)	Amanda Bowe (Post Office Insurance ARC Chair): Item 8
Alisdair Cameron (Group CFO)	Jeff Smyth (Interim Group CIO): Item 9
Ben Foat (Group General Counsel)	Tony Jowett (CISO): Item 9
Andrew Paynter (Audit Partner, PwC)	Joseph Moussalli (Programme Manager): Item 9
Sarah Allen (Senior Manager, PwC)	Rob Wilkins (Cloud Services Director): Item 9
Johann Appel (Head of Internal Audit)	Sarah Gray (Group Legal Director): Items 10, 11 & 12
Mark Baldock (Head of Risk)	Hugo Sharp (Deloitte Partner)
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	

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

Time		Item	Owner	Action
09.00	1.	Welcome & Conflicts of Interest	Chair	Noting
09.05	2.	Policies for Approval	Jonathan Hill	Approval
		2.1 [Procurement Policy]		
		2.2 Contract Execution		
		2.3 Vulnerable Customer		
		2.4 Physical Security		
		2.5 HMRC Fit & Proper		
09.15	3.	Previous Meetings	Chair	Approval
		3.1 Minutes (20 July 2020)		
		3.2 Action List		
		3.3 Draft Risk and Compliance Committee Minutes (10 September 2020)		
09.20	4.	Deepdive: Successfactors	Lisa Cherry/ Daisie Jope	Noting and Approval
09.35	5.	Pensions Assurance – RM Pensions	Maxine Cross	Noting and Approval

13

Strictly Confidential

POL00401629

POST OFFICE LIMITED

09.50	6.	Post Master Accounts	Tim Perkins	Noting and Approval
10.00	7.	Corporate Insurance Renewal	Mark Dixon/ Andy Bear	Noting and Approval
10.10	8.	Update from Subsidiaries: verbal update Post Office Management Services (ARC)	Amanda Bowe	Discussion & Noting
10.15	9.	PCI-DSS and Cyber Security Update	Jeff Smyth	Noting
		9.1 PCI-DSS	Jeff Smyth	
		9.2 Cyber Security	Tony Jowett	
		9.3 Joiners, Movers, Leavers	Tony Jowett	
10.30	10.	Bi-Annual Legal Risk Review (Non GLO/ Starling)	Sarah Gray/ Ben Foat	Noting
10.40	11.	Law & Trends Update	Sarah Gray/ Ben Foat	Noting
10.50	12.	Contract Management Framework	Sarah Gray/ Ben Foat	Noting
11.00	13.	Consolidated Report from Risk, Compliance and Internal Audit		
11.00		13.1 Risk Report	Mark Baldock	Noting
11.10		13.2 Compliance Report	Jonathan Hill	Noting
11.20		13.3 Internal Audit Report	Johann Appel	Noting
11.30	14.	Any other business	All	Noting
Next ARC Meeting: Tuesday 24 November 2020 at 09.00 to 11.30 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ				

13

Strictly Confidential