POL00423569

POST OFFICE LIMITED

Meeting:	Risk and Compliance Committee
Date:	6 May 2020
Time:	14.00 - 17.00
Location:	Via Microsoft Teams

Present:	**Attendees:**
Alisdair Cameron (Chairman)	Johann Appel (Head of Internal Audit)
Nick Read (Group CEO)	Mark Baldock (Head of Risk)
Ben Foat (Group General Counsel)	Jonathan Hill (Compliance Director)
Amanda Jones (Group Retail and Franchise Network Director, Interim)	Tom Lee (Head of Finance Financial Accounting and Controls)
Andrew Goddard (deputising for Owen Woodley)	Rebecca Whibley (Assistant Company Secretary)
Lisa Cherry (Group Chief People Officer)	Tony Jowett (Chief Information Security Officer): Item 5
Jeff Smyth (Group Chief Information Officer, Interim)	Sherrill Taggart (Interim Legal Director): Items 6 & 7
Julie Thomas (Operations Director)	Barbara Brannon (Procurement Director): Item 8
	Rod Williams (Head of Legal DR & Brand): Item 9
Apologies:	
Owen Woodley (Group Chief Commercial Officer)	
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 (9 March 2020)		Approval
		2.2 Action List		Discussion
14.15	3.	Combined Risk, Compliance and Audit Update		
		3.1 Risk Report, including update on internal controls software	Mark Baldock	Noting (onward submission to ARC)
		3.2 Compliance Report, including the Mails Dangerous Goods Compliance Action Plan	Jonathan Hill	Noting (onward submission to ARC)
		3.3 Internal Audit Report	Johann Appel	Noting (onward submission to ARC)
14.45	4.	Internal Audit Plan 2020/21	Johann Appel	Noting (onward submission to ARC)
15.00	5.	PCI-DSS and Cyber Security Update		
		5.1 PCI-DSS, including broader Fujitsu relationship	Jeff Smyth	Noting (onward submission to ARC)
		5.2 Cyber Security	Tony Jowett	
15.15	6.	Progress Update on the Pilot Implementation of the Contract Management Framework	Sherrill Taggart	Noting & Approval (onward submission to ARC)
15.30	7.	Horizon Scanning Update	Sherrill Taggart	Noting (onward submission to ARC)

POL00423569

POST OFFICE LIMITED

15.45	8.	Supplier Contracts out of Governance	Barbara Brannon	Noting
16.00	9.	Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy	Ben Foat / Rod Williams	Noting (onward submission to ARC)
16.15	10.	Review of draft Audit, Risk and Compliance Committee (ARC) meeting agenda 19 May 2020	Chairman	Noting
16.30	11.	Any other business	Chairman	Noting
Next RCC Meeting: Monday 13 July 2020 at 14.00 to 17.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ				

POL00423569

Post Office Limited Risk and Compliance Committee Actions
Updated: 30.04.2020

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
RCC Meeting 14.03.20					
3.3 - Cyber Security	Internal audit would be commissioned to complete an audit on FRES (subject to approval in the master services agreement).	BF	TBC	Sherrill Taggart has asked the Legal Team to review the FRES contract.	**Open**
3.3 - Cyber Security	Updated guidance has been issued by the National Cyber Security Centre (NCSC) on how to defend against an attack. The Committee requested this guidance be circulated to the GE and Board.	TJ	06/05/2020	Regarding Social Media and how we should go about hardening, the NCSC guidance referenced in the meeting is at https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely An update on this is also provided in the Cybersecurity update paper for 06/05/2020. Veronica Branton (Company Secretary) to share guidance with the Board.	**Open**
4.12 Combined Risk, Compliance and Audit Update	**Responses to formal Ofcom information requests –** the Committee was informed of issues with the accuracy of information provided by third party suppliers following formal s136 and s137 information requests. The Committee questioned how the accuracy of data requested could be improved and what safeguards POL had in place to check accuracy. JS would co-ordinate a response.	JS	06/05/2020	Compliance is working with the Telecoms Team and Fujitsu to correct the inaccuracies of previous submissions and improving accuracy of all future submissions. The key area to improve is the transparency of the Fujitsu data preparation so that it can be checked by Post Office. Fujitsu has been asked to work with its suppliers (BT and TT) to enable additional cross-checking of data. We now seek a formal sign-off from Fujitsu on the integrity of the supplied data.	**Recommended for closure**
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	06/05/2020	These issues have not been raised previously to the Committee or to ARC.	**Recommended for closure**
RCC Meeting 14.01.20					
6.18 - Payment Services Directive 2 (PSD2) Implementation	Payment Services Directive 2 (PSD2) Implementation – submit letter to regulator	MS	ASAP	Completed	To close

POL00423569

Post Office Limited Risk and Compliance Committee Actions
Updated: 29.04.2020

10.6 - Money Laundering Reporting Officer (MLRO) Annual Report	BF, SS and JH talk to retail on enforcing three lines of defence and suggested BF attend a meeting with HMRC.	SS/JH			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.	CM/Marketing		In progress – subject to PSG funding.	Open
3.3 Supplier Contracts out of Governance	Brands/RAPP – Agree date for tender	SH/Marketing		In progress – subject to PSG funding.	Open
4.1 PCI-DSS Update	Circulate final pricing and deadlines document from Ingenico	SH	January 2020	In progress. Update to be provided in PCI-DSS verbal update.	Open
5.3 Cyber Security	A major incident test be completed with findings reported to the Committee.	TJ	January 2020	Update to be provided in Cyber Security update paper.	Open
5.3 Cyber Security	Joiners/movers/leavers – to review whether contractors who no longer work for POL have been removed from POL emails and systems.	DZ/LC	January 2020	A paper is to be presented to GE.	To close
5.3 Cyber Security	Joiners/movers/leavers - A routine cycle of checking third party access to be implemented.	TJ	January 2020	Update to be provided in the Cyber Security update paper.	To close
5.3 Cyber Security	Joiners/movers/leavers - IA to review end to end process of joiners/mover/leavers as part of the 2020/2021 IA audit plan.	JA		JML has been added to the 2020/2021 IA plan.	To close
6.14 Internal Audit	**Data and Analytics Excellence (Programme Assurance) –** AC advised the management comment would be reviewed for clarity.	AC/SH	25 November	Report Updated for ARC	To close
7.5 Contracts Management Framework	It was **AGREED** a discussion on contract management would be held at GE.	BF		Discussion held at GE.	To close

POL00423569

Post Office Limited Risk and Compliance Committee Actions
Updated: 29.04.2020

RCC Meeting 03.09.19					
5. Compliance	GDPR – Contracts To identify contracts requiring GDPR remediation, the majority of which are IT service contracts with no owner identified.	Barbara Brannon and Shikha Hornsey	November 2019	This is in train for completion by 31 March 2020.	Open

Strictly Confidential

POL00423569

2

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE

Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 09 March 2020 at 14.30 pm

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
	Stephen O'Reilly (SR)	HR Director - Business Partnering & Recruitment (deputising for Lisa Cherry)
	Jeff Smyth (JS)	Group Chief Information Officer, Interim
	Julie Thomas (JT)	Operations Director
	Owen Woodley (OW)	Group Chief Commercial Officer
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
	Sherrill Taggart (ST)	Legal Director, Interim
	Barbara Brannon (BB)	Procurement Director
	Andy Kingham (AK)	Head of Network
	Karl Oliver (KO)	Head of Commercial Partnerships
	Mark Dixon (MD)	Head of Treasury, Tax & Insurance
Apologies	Nick Read, Group CEO	
	Lisa Cherry, Group Chief People Officer.	

1. Welcome and Conflicts of Interest **Actions**

1.1 AC opened the meeting and advised that papers would be taken as read.

1.2 The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

2. Minutes and Action Lists

2.1 The minutes of the RCC meeting held 14 January 2020 were **APPROVED**.

2.2 Progress on completion of actions as shown on the action log was **NOTED.**

3. Cyber Security

3.1 TJ provided an update on Cyber Security. Security maturity was on track and the team planned to close as many actions before the end of March when Deloitte would be completing a reassessment exercise. An audit would be completed in April/May on progression. IA believed the work to date was slightly behind schedule.

3.2 **Ransomware** - Since the Travelex attack, greater team focus had been on ransomware attacks which he noted were becoming an increasingly serious threat. FRES has now provided written assurance that its defence systems are suitable for purpose against ransomware attacks, and a diagnostic exercise is planned for mid-March by Deloitte to develop a playbook for use in the event of an attack.

3.3 Internal audit would be commissioned to complete an audit on FRES (subject to approval in the master services agreement). **BF**

3.3 Updated guidance has been issued by the National Cyber Security Centre (NCSC) on how to defend against an attack. The Committee requested this guidance be circulated to the GE and Board. **TJ**

3.4 Regarding an insider threat attack, a red team exercise completed using social media to identify and target people who could be approached for internal access, identified names, addresses, contact details and

POL00423569

family photographs of Board and senior and members of staff. Guidance from the NCSC would be circulated to Board and GE members reminding senior members of staff on the importance of safe usage of IT and social media platforms. He noted there was limited control from top-down access.

3.5 The Committee discussed 3rd party IT controls and outsourced IT controls, noting a positive change in behaviour and sought to understand whether POL had a right to audit.

3.6 **Joiners, Movers, Leavers** – good progress has been made and a plan developed, however there are integrity issues between systems (Successfactors, Active Directory and NIM) leading to a lack of alignment regarding data/information. Q1 would see some work to tighten-up work standard access and 3rd party access, but that there are no issues with privileged access.

3.7 **Telephone Security** – it was noted this would be reviewed by JH, Sally Smith and Martin Kearsley.

4. Combined Risk, Compliance and Audit Update

Risk

4.1 The current top principal risks (based purely on their RAG status) were PCI Compliance, Group Litigation, Retail Proposition and Telco. The two key subsidiary business risks were Coronavirus (Covid-19) and Digital Identity both of which were noted.

4.2 The Committee noted that the Central Risk had embarked on a top-down refresh/update of the enterprise (formally principal) risks and the intermediate (formally business) risks. This was supported by a facilitated GE session in February. The output of this work (around 14 enterprise risks and 55 subsidiary intermediate risks) is being finalised and uploaded onto the corporate GRC (governance, risk and compliance) Tool (Archer). Going forward, and subject to the deployment beyond the Central Risk team, Archer will provide POL with a single source of truth with respect to its enterprise and business risks.

4.3 In terms of the key change programmes:

4.4 **PCI Compliance** – the project remains "Red" overall against current plan however there is increased focus on driving the status back to green. As Baseline delivery plans and costs was received at the end of February 2020, this is likely to result in an improved status in the next reporting period.

4.5 **Group Litigation** – although the project remained 'Amber' overall, the team was confident spend and benefits would remain within 2019/20 budget. Any underspend would flow through to 2020/21.

4.6 **Retail Proposition** – agents consider POL too costly, complex and unattractive to join, however it was felt the increased agent remuneration would improve branch sustainability.

4.7 **Telco** – as the sector was becoming increasingly regulated, there is the risk that the business becomes partially or fully non-compliant.

4.8 **Coronavirus** – the risk has been raised in line with government recommendations. A rapid response team has been established to walk through scenarios and identify any risks/gaps.

4.9 **Digital Identity** – alternative partnership and business models are being explored. The existing contract has been extended up-to November 2020 and negotiations are underway.

Compliance

4.10 **Ofcom Text Relay** – the Committee was made aware that POL has now paid the £175K fine regarding Text Relay. The issue has now been officially closed.

4.11 **Ofcom Fairness** – Ofcom has expressed concern with Telco's drive of providers being 'fair', noting that POL has the largest percentage of out of contract customers relative to its customer base. Telco is reviewing all options as we have committed to the fairness principles especially as the End of Contract and Best Tariff notifications are expected to have material impact on our customer retention.

4.12 **Responses to formal Ofcom information requests –** the Committee was informed of issues with the accuracy of information provided by third party suppliers following formal s136 and s137 information requests. The Committee questioned how the accuracy of data requested could be improved and what safeguards POL had in place to check accuracy. JS would co-ordinate a response. **JS**

4.13 **Consents Guidance (Use of Cookies) –** the Committee was reminded of the updated guidance published by the regulator on the use of data cookies on websites. POL is partially compliant and work is underway to ensure full compliance in April 2020.

4.14 **Gifts and Hospitality –** staff members continued to receive cash gifts and whilst training was in place, accountability was not enforced. The Committee asked the team to investigate would could be done and suggested a three tiered approach of initial warning from line manager, letter on file, dismissal.

Internal Audit

4.15 The following points were raised:

4.16 JA reported good progress had been made with the audit plan for 2019/20 with six audit reviews finalised since the last Audit Risk and Compliance Committee (ARC) meeting (28 January 2020), these being Branch

POL00423569

Banking Services, Accounts Receivable, Investment Funding Controls, Supply Chain CViT, Data Privacy and HIH Programme Assurance.

4.17 Four of the audits reported 'Yellow' (Branch Banking Services, Supply Chain CViT, Data Privacy, HIH Programme Assurance) and two 'Green' (Accounts Receivable, Investment Funding Controls). There is one overdue action over 60 days regarding FS Training (Branch Sales). A new action owner has made progress however the policy requires additional clarity and approval. It is expected this will be completed by 30 April 2020.

4.18 With regards to the Data Privacy audit, although there were a high number of audit findings (13 in total), the audit was rated "Needs Improvement" as these were mostly low priority process improvement type findings. IA and the Deloitte (co-source provider) both felt that controls were generally fit for purpose and comparable with organisations of similar size and complexity.

4.19 JA was pleased with the progress made to date on the IA plan 2019/20. He believed the team would be able to complete the IA plan before May's Audit, Risk and Compliance Committee (ARC) meeting.

5. Internal Audit Plan 2020/21

5.1 JA presented the IA plan for 2020/21. The plan consists of 26 audits in total, 18 internal control reviews and eight change/programme assurance reviews. Six audits are also planned for Post Office Insurance.

5.2 The Committee noted the co-source requirement to deliver the plan was 422 days at a cost of £431K.

5.3 Regarding the Internal Audit for GLO Operations, the Committee noted that some of the other IA's would be indirectly linked to this. AC requested the GE sponsor for Post Master Reporting be checked.

6. Annual Legal Risk Report 2019/20

6.1 BF and ST presented the annual legal risk report for 2019/20 advising of the following key legal risks:

- Contract Management (Financial)
- Regulatory Compliance (Regulatory)
- Corporate acquisitions/disposals and JVs (Strategic)
- Dispute Resolution (Litigation)
- Intellectual property and trade mark (Reputational)
- People and processes (Operational).

6.2 The Committee discussed the following key legal risks:

6.2 **Contract Management –** good progression has been made in improving contract management governance within the group, however culture and accountability remains a stumbling block. Contract owners should be held accountable for the management of the contract, and should not delegate this obligation to other members of staff.

6.3 Following a request from ARC, an exercise has been completed to identify the top material contracts in terms of financial and strategic risk, which will be presented to ARC for review in March. It was noted that contract management has been listed as part of the IA 2020/21 plan, however the Committee questioned the post control impact assessment rating of 'Green'.

6.4 The Committee noted that Contract Management was listed in the IA 2020/21 plan and questioned the post control impact assessment rating of 'Green'.

6.5 **Competition Law** – following the acquisition of Payzone Bill Payments Limited (PZBPL) , the legal team has provided advice/guidance on sharing commercially sensitive information 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.

6.6 The Committee questioned whether these examples had been flagged to the Committee or ARC before? **DP**
[Post meeting note – these issues have not been raised previously to the Committee or to ARC.]

6.7 **Corporate M&A, Disposals and RfPs** – the Committee questioned the inclusion considering POL's limited activity in this area. ST advised there had been activity during 2019/20, however the legal risk centred around the lack of internal expertise (relating to M&A activity), which may mean that anticipated returns are not met.

6.8 The Committee requested the Post Control Impact Assessment ratings be more clearly narrated.

7. Contract Management Framework

7.1 The team had identified 142 material contracts (following a request from ARC to identify key financial and strategic contracts) and these have now been allocated to, and agreed by GE and GE-1 members. 104 of the 142 material contracts have 36 identified contract owners. 26 of the 104 contracts have current signed contracts in place that can be located, and these 26 material contracts are managed by a pool of 17 confirmed contract managers.

DRAFT

POL00423569

7.2 Work had commenced to populate Web 3.0 (Source to Settle, the platform hosting the contracts) and training will be provided to individuals responsible for material contracts once an external training provider has been procured.

7.3 Noting that some contract managers had large numbers of contracts allocated against their name, BF reiterated the importance of contract managers being comfortable with this (due to the risks involved).

8. Supplier Contracts out of Governance

8.1 BB reported there had been 4 new non-compliant incidents since the last Committee meeting (14 January 2020). Overall, non-compliance has risen from £20.2m to £21.01m, primarily driven by new high value direct awards assessed as Low Risk, which fall under Regulation 32 exemptions. The following contracts were discussed as low risk:

8.2 **New Award** – this is an £371,000 award for the provision of benchmarking services for UK competitors in financial services, mortgages, loans, credit cards etc. This is assessed as low risk under PCR Regulation 32 due to the lack of market competition.

8.3 **NCR –SSK Support** – this is a contract extension valued at IRRELEVANT The software and hardware can only be provided by the manufacturer/owner of the intellectual property rights (IPR). This is assessed as low risk under PCR Regulation 32 on IPR grounds.

8.4 **Cardew Group** – this is a contract extension valued at IRRELEVANT for the use of PR services relating to GLO.

8.5 **Space Between:** this is a contract extension valued at IRRELEVANT for the provision of conversion rate optimisation services (i.e. conversion of website visitors to customers). The compliant tender process for the replacement supplier has been completed and the contract awarded. Service cutover is planned for April.

8.6 The Committee discussed the following contracts in the pipeline considered high-risk:

8.7 **EUC** – this is a IRRELEVANT project initiated to re-procure End User Computer services for branch and colleague services. New suppliers are planned to be in place before the expiration of the current contract (April 2021) and is gathering requirements to go to market. BB felt this was achievable due to the intent to insource some key IT activities.

8.8 **Media Planning** – this is an £1.5m contract due to expire in April 2020. The preferred business strategy is to re-procure via OJEU and expand the scope to include Media Buying valued at £20m. It was noted that although compliant, supplier performance had been unacceptable and combining the two services is not an available option under the CCS frameworks and an OJEU would enable a supplier of both to bid for the work. The tender process is already underway.

8.9 **Brands/RAPP** – this is an IRRELEVANT contract extended to April 2020. A business strategy, funding and sourcing plan needs agreement.

8.10 **Global Payments** – this is an IRRELEVANT contract due to expire in May 2020. An extension would be required for 12-24 months until a new provider can be found. A discussion has been held in GE (January 2020) to discuss all options. It was noted that if the Board turned the contract down, this could have implications for the PCI-compliance programme.

9. Selling Regulated Products in the Branch Network

9.1 AK and AJ presented a report on Selling Regulated Products in the Branch Network.

9.2 AK reported that whilst selling products in isolation was not difficult per se, the challenge was selling c.120 products whilst keeping product knowledge and operational understanding up-to-date. He believed the network sales processes required simplification whilst remaining compliant and advised that most product failures were due to lack of understanding of products and the failure to follow processes.

9.3 In terms of network governance controls, there are regular mystery shopping exercises, three monthly forums to review risk, management information and conduct risk, and a team of nine area managers has been established to provide training and champion conformance across the network.

9.4 The Committee questioned whether it would be more effective to switch off/stop the sale of products by repeat offenders and the consequences of doing so. AK responded that he believed that conformance levels would only improve (particularly in locals) once the number of products for sale had been decreased. Additionally, he felt the customer journey process should also be simplified.

10. Partner Failure Contingency

10.1 KO and AJ provided an update on partner failure contingency.

10.2 KO reported that since November (where McColls was flagged as vulnerable), the team had developed a 'Partner Failure Response' plan identifying the immediate actions that would be taken to mitigate/reduce risk in the event of a partner collapse.

POL00423569

10.3 He advised that a rapid response team had been established, with operational plans involving a cross-functional team developed. Additionally, the team had successfully conducted a dummy workshop exercise to run through the expected response of a partner collapse.

10.4 In the event of a partner collapse, it was noted that sites would be re-opened via a staggered process with priority given to :

1. branches where the nearest neighbouring branch was not within 1 mile (urban deprived), 1.5 miles (urban) or 3 miles (rural), with low replace ability (lack of replacement sites in the local area) and secondly, where the nearest neighbouring branch is not within 1 mile (urban deprived), 1.5 miles (urban) or 3 miles (rural) with replacement sites available.
2. Branches where the nearest neighbouring branch is not within 1 mile (urban deprived), 1.5 miles (urban) or 3 miles (rural) with replacement sites available.

10.5 The Committee questioned whether in the event of a partner collapse, Payzone been included in the mapping exercise? KO explained that the team had reviewed all available and alternative solutions, such as the "Post Office on Wheels", using Payzone sites and establishing a POL owned subsidiary that would act as an interim post master agent, utilising existing McColl's staff to operate the branch.

10.6 It was noted however that although the alternative solutions could provide the majority of Post Office services, they could not provide all of them.

11. Policy for Approval – Treasury Policy

11.1 The Treasury policy was **APPROVED** for submission to the ARC on 24 March 2020.

12. Review of draft Audit, Risk and Compliance Committee meeting agenda

The draft ARC agenda for 24 March was **NOTED**.

13. Any other Business

There was no other business.

DRAFT

POL00423569

POST OFFICE LIMITED RISK & COMPLIANCE COMMITTEE REPORT

3

Title:	Risk, Compliance and Audit Report	**Meeting Date:**	6 May 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, specifically:
   - the status of the current enterprise risks and intermediate risks
   - the status of the current COVID-19 risk position
   - the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer)
   - the status of the Change Portfolio and key delivery challenges.

2. Note the Compliance update, the impact of Covid-19 on the approach to compliance, the deferment of the HMRC branch registration fees and the update on the Mails Dangerous Goods Action Plan.

3. Note the progress being made with delivery of the Internal Audit programme and completion of audit actions.

Confidential

POL00423569

3

Risk

Questions addressed

1. What are the Post Office's current enterprise risks and key intermediate risks?
2. What is the Post Office's current COVID-19 risk position?
3. What is the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer)?
4. What is the status of the Change Portfolio and key delivery challenges?

The Post Office's current Enterprise and key Intermediate risks

1 In February 2020 we facilitated a GE session to look at the key business risks currently faced by the Post Office. This review resulted in the identification of **15** active enterprise risks and **54** linked intermediate risks. This refreshed data set replaced, what were formerly termed, the Post Office 'principal' risks.

2 The **15** enterprise risks mirror the HM Government's approach to enterprise risk classification[1]. As such they are grouped around such themes as Strategy, Operational, Financial, Legal etc. The Health & Safety enterprise risk was articulated to cover a number of potential incidents including adverse physical attacks as well as a pandemic. Given the current context we have disaggregated this particular risk and articulated a separate (and more comprehensive) COVID-19 risk data set which is discussed later in this paper.

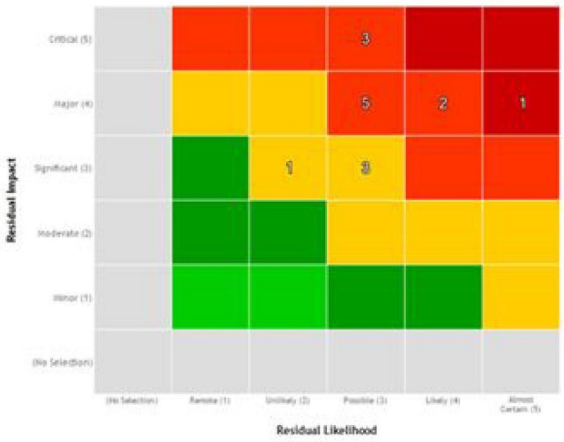


Figure 1: Post Office enterprise risks: April 2020

3 The key enterprise risks (excluding Health & Safety) are:

- **Commercial (4:4)**: the Post Office's commercial proposition may be unattractive because the existing products are too complex or confusing, new products are cost ineffective, unable to be scaled and unattractive to the market. In part prompted by the Post Office's COVID-19 response a review is now underway to consider what the business should look like in the medium and long-term. It will include identifying what Markets are critical to us and the supporting operational functions key systems, policies etc needed to support us.

[1] HM Government: Management of Risk (Principles and Concepts) – June 2019

POL00423569

- **Legal (4:3)**: the Post Office may be unable to comply with legislative and regulatory changes. Workstreams in place including the GLO programme to manage the current and ongoing post-litigation work
- **Financial (5:3)**: Because of the unpredictability of income and expenditure there is a risk that the Post Office has insufficient funding and/or uncontrolled costs in the short-, medium and long-term
- **Technology (5:3)**: the Post Office is heavily reliant on third party suppliers and has an ageing IT infrastructure on both hardware and software components.
- **Marketplace (4:3)**: Post Office services and products across the various sectors may decline and/or loyalty to the Brand reduce resulting in loss in attractiveness for sub-postmasters, loss in revenue and reputational damage

4 Our key intermediate risks (which lie below enterprise level) include:

- **Commercial (Government Services) (5:4)**: Risk the Post Office's revenue from the provision of Government Services (i.e. Digital Check & Send, IDPs) reduces over the short-, medium- and long-term
- **Commercial (Customers (Physical Service) (5:4)**: Risk the Post Office's long-term customers want to continue to access increasingly less cost effective physically-served products and series
- **Financial (Digital Income) (5:4)**: Risk the Post Office on-line products and services generate a reduced income level compared to comparable physical products and services
- **Marketplace & Brand (Customer Demand) (5:4)**: Because of the evolution of the Retail and Consumer sector, there is a risk the 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 in loss in revenue, sustainability and reputational damage
- **Technology (IT Infrastructure) (4:3)**: The existing IT infrastructure, hardware and software is inadequate or approaching end of life

5 Appendix **1** provides further detail.

6 It is clear the Post Office COVID-19 risk identification and management activity now needs to be fully assimilated into our wider enterprise risk work. This may result in some re-articulation of a number of the non-COVID-19 enterprise and intermediate risks, their likelihood and severity assessments and associated mitigating actions. This was to be expected as ongoing separation would have been artificial. This alignment and assimilation work will be the focus of the next reporting period. It will involve widening the scope of our COVID-19 KRI and risk appetite statement work to cover wider enterprise risk activity.

COVID-19

7 Since the last RCC/ARC Central Risk have led urgent work on identifying all key COVID-19 related operational risks. The work was undertaken in two Phases. Phase 1 was an industry-wide and sectoral analysis (international and domestic) of the typical COVID-19 emerging risks we were likely to encounter and was completed on 31 March. We quickly followed this with Phase 2. This involved detailed discussion with key individuals within the business to confirm the relevance (or otherwise) of these typical risks, tailoring them as required and then assessing their respective impact, likelihood and proximity.

POL00423569

8 We concluded we have **1** single overarching COVID-19 enterprise risk, **13** intermediate thematic risks (operational, strategy, legal, financial etc) and **56** specific low level risks. A comprehensive summary is provided at Appendix **2**. Our critical low-level risks are

- **Change (4:5)**: may have insufficient change funding available to deliver our planned change activity
- **People (4:4)**: Post Office frontline staff could get infected with COVID-19 by customers visiting branches to perform various counter transactions
- **People (4:4)**: significant number of Post Office employees could become stressed, fearful, overwhelmed and isolated because of social distancing etc
- **Commercial (4:4)**: Post Office short-term business-critical activities, products, services, business processes and systems have a high dependency on third parties who could have a high degree of COVID-19 risk exposure
- **Financial (4:4)**: Post Office will face months of exceptionally poor trading conditions with immediate lost revenue potentially representing a permanent loss putting unanticipated pressure on liquidity

9 Of the **56** low-level risks we estimate **27** (50%) could materialise in the short term (within a month), **17** (31%) in the medium-term (within 3 months) and **10** (19%) (over 3 months) in the long-term – but only <u>if mitigations were not proactively identified or delivered</u>. All risks have mitigation plans identified and owners and dates. We have seen a clear trend in the short-term risks being managed closer to Target RAG after which further mitigations will not be required. These risks will simply be monitored thereby freeing up resource.

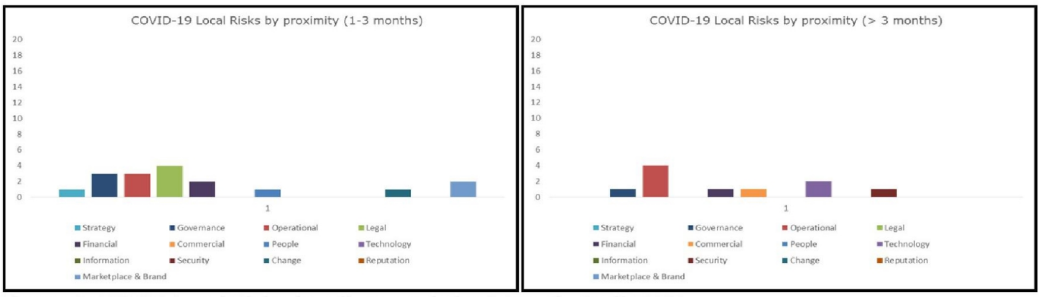


Figure 1: COVID Local Risks (medium- and short-term): April 2020

10 Our key medium-term risks include **Strategy** (Unclear Target Operating Model), **Finance** (Cash-insufficient facility and security headroom) and **Change** (insufficient funding). Key long-term risks include **Commercial** (Long-term declining sales & demand) and **Technology** (Inability to grasp future digitalisation).

11 The highest number of risks are Operational (**18**) with Governance (**6**) and People (**6**) the next highest. Change, Commercial and Financial have less risks in number but tend to have proportionally higher-rated risks.

Confidential

POL00423569

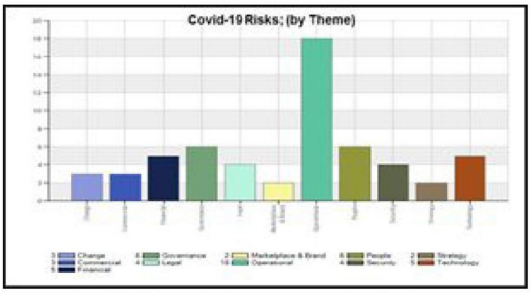


Figure 2: COVID risks by theme (April 2020)

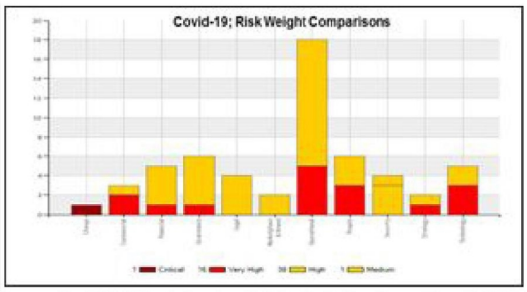


Figure 3: COVID risks by RAG distribution (April 2020)

12 We have initiated a fortnightly reporting cycle (tightening mitigations, clarifying ownership, reporting slippage etc) allowing us to report (in almost real-time) to the COVID-19 SteerCo. We are finalising a draft set of COVID-19 KRIs and an associated risk appetite statement. The aim of this work is to secure, going forwards, agreement on how tolerant/averse/seeking we are thereby helping prioritise resource. Finally we are providing input to Project NEO around medium/long-term proximity risks to ensure their emerging work plan mitigates the impact and likelihood of these risks.

13 Appendix **2** provides further detail.

The implementation of the Post Office's Governance, Risk & Compliance (GRC) tool (Archer)

14 The Central Risk team have embarked on implementing Archer (an industry standard GRC tool) to enhance the efficiency of our risk management. We have successfully uploaded the

- refreshed set of non-COVID-19 enterprise risks and their linked business (intermediate) risks and the complete COVID-19 risk data set (enterprise, intermediate and local records). The graphical analysis in this report is derived directly from Archer.
- complete set of open Risk Exceptions

15 We are now continuing with our top-down approach and are about to commence the phased deployment of Archer across the Group Commands all the time making sure any lower level risks (where appropriate) align and link to the higher level enterprise and business risks.

The status of the Change Portfolio, including top risks and key delivery challenges?

16 By the end of March 2020 the overall status of the Portfolio remained Amber. As a result of COVID-19 the Portfolio is being reviewed to reduce the amount of non-critical activity and control spend. Options will be presented to the Board in May 2020.

17 The March 2020 spend was £21.9m with full year spend equating to £222.4m (including GLO). The benefits achieved in March 2020 were £7.1m with a full year total of £59.5m. Both the year–end spend and benefits figures are under final review and may change. The 2020/21 benefit position is subject to re-prioritisation and agreement of baseline position by the Board.

18 Since the last RCC/ARC there has been a decrease (from 7 to 4) in the number of gold and platinum projects reporting an overall Red RAG status:

POL00423569

- IDS Digital Identity: Marked as Red prior to business case approval to detach In-Branch Verification from the Digital Identity parent. Once detachment occurs closure of the Digital Identity project can go ahead. A business case was reviewed by Portfolio Review Board, however further detail is required.
- Project Starling: Cost increased from changing law firms. Exact funding is still to be approved. Options to reduce spend are being investigated
- PCI (Compliance): The Red status had been given due to Programme delivery remaining Red. Integrated programme plans currently indicate delivery completion in August 2021. Further work continues with suppliers to see if this can be brought forward.
- Digitising Mails (Cost, Benefits and Overall Red RAG): Project on hold until completion of Royal Mail negotiations and McKinsey's due diligence work on our overall Mails strategy.

19 Appendix **3** provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status.

Compliance

Telecoms

Telecoms provider response to Coronavirus

20 Telecoms voice services are considered by government and Ofcom to be a lifeline service as they enable customers to make calls to emergency services and stay connected during this period of isolation. In support of this the telecoms team has;

- Prioritised fault repairs for vulnerable customers at its call centres during the lockdown.
- Stopped non-critical activities such as sales to enable focus to be on supporting existing customer issues.
- Equipped call-centre staff for home-based working, which has enabled us to maintain a stable service and manage staff absences

21 Ofcom is monitoring all providers' support of vulnerable customers. Like other providers, at Ofcom's request we are providing a weekly update on the status of our service provision and highlighting any issues that may arise.

- Ofcom is concerned that providers are suspending End of Contract notifications ("ECNs"). ECNs were putting our contact centre under strain, with reduced staff numbers due to Covid-19, inhibiting our ability to service vulnerable customers. However, together with directing customers to our online self-care portal and improved contact centre capacity we have advised Ofcom that we will keep sending ECNs.

22 The Department of Culture Media and Sport (DCMS) oversees telecoms regulation in the UK. As part of the government response to the coronavirus outbreak it has asked a number of the UK's largest telecoms firms to make commitments, which include:-

- Free and low cost calls for vulnerable customers
- Working with customers who maybe struggling with debt
- Removal of data caps

POL00423569

- Priority faults repairs for those who are self-isolating or an alternative means of communication
- Support NHS workers and services through certain enhancements, including priority broadband upgrades for NHS clinicians at home who may provide consultations or upload large files.

23 We met with DCMS staff on 24th April to discuss what we are doing to support customers. We have been asked to sign up to the DCMS commitments. Initial dialogue with DCMS indicates that we are satisfying these but we are going through the details with them to confirm.

PSD2

24 In January 2020 Post Office wrote to the FCA to inform it of our intention to seek an Electronic Communications Exemption ("ECE"). This requires Post Office to cap premium rate calls at £40 per call and £240 per month in aggregate. We informed the FCA that we would repay any over charged customers going back to when the obligations came into effect on 13th January 2018. The FCA confirmed it was happy with our approach.

25 The PSD2 work has been split into 3 phases:

- Phase 1 was to repay customers who had been overcharged between January 2018 and February 2020. This has now been completed.
- Phase 2 is to create an interim solution to enable us to reimburse customers going forward who incur charges over the caps in the previous billing month. This is only a partially compliant solution and is underway now.
- Phase 3 will deliver Post Office a compliant solution by enabling us to credit customers for any overcharge in the same billing month. By the end of April 2020 we expect Fujitsu to confirm this solution can be implemented and a delivery date. We will then update the FCA with our progress and seek to apply for an ECE.

European Electronic Communications Code

26 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.

27 The required implementation date is 21st December 2020

- Most UK providers believe this timescale is unrealistic and responded to Ofcom stressing this point. Ofcom has indicated that this is a mandate from DCMS, which has only very recently confirmed to the industry that it still expects providers to meet the timeline. The industry will continue to ask for more time as a minimum, not least because of the significant investment telecoms providers are directing to supporting customers though Coronavirus, including the additional commitments that providers have been asked to sign-up to by DCMS.
- Compliance is working with the Telecoms Team on plans to comply with EECC but this is a challenge for the business both in terms of budget and a lack of clarity on the obligations from Ofcom.
- Ofcom is now planning to publish clarification on the majority of the EECC obligations in Q2 and EECC "switching" obligations in Q3/4 2020/21, which would make compliance

POL00423569

with the obligations very difficult. To be fair to Ofcom, it is discussing implementation dates with DCMS.

Data Protection

Support for Post Office Businesses during the COVID 19 pandemic.

28 Our key objective is to ensure that the new ways of working do not compromise Post Office's ability to meet it regulatory obligations whilst at the same time being as flexible as possible and trying not to place an undue burden on the ability of the business to meet the Coronavirus crisis. New processes include, but not limited to:

- HGS, POCA and NBSC operating call centres from home.
- Printing from Home, this was up and running within 36 hours
- Easy Cash
- Easier to implement Delegated Authorities for Telco users.
- Support to POL Identity team to allow back-end system access to clear backlog of Digital Identity application.

Update from Meeting with the Information Commissioners Office (ICO Data Protection Regulator 14th April):

29 The key objective of this meeting was for the ICO to outline its expectations during the Covid-19 crisis. The key takeaways were:

- Its business as usual. However, the ICO will be sympathetic to organisations that are having to implement new processes for home working where due diligence may not be as stringent as usual.
- Organisations that attempt to meet statutory deadlines for dealing with Information Rights requests such as Data Subject Access requests and Rights to Erasure will not be penalised for missing delivery dates. To date, Post Office has missed no deadlines as a result of Covid-19 restrictions.
- Organisations will still be expected to report breaches within 72 hours but the ICO accepts that remediation and investigation work may take longer to complete due to offices being closed and staff absentee rates being high. Post Office has asked for and received a relaxation on the 24 hour PECR reporting requirement to 72 hours.
- Administrative areas of UK DPA such as Privacy Impact Assessments and Record of Processing Activities can be retrospectively completed for processes being introduced to accommodate home working.

Post Office use of Cookies on Internet and Apps

30 A proposal for resolving the outstanding Cookies issue has been built and been deployed on the Post Office website. However, the solution requires further development to position Post Office "in the pack".

31 To be within Risk Appetite the Digital team will develop the functionality that allows users to change their cookie settings as easily as it was to apply them. The Digital team believes this can be achieved within 2-3 weeks but are currently constrained both by limited budget and Covid-19 priorities.

POL00423569

Data Protection Incident – Loss of HR Files

32 As a result of a Data Subject Access Request by an ex-employee an investigation has found that at least 13 boxes of Personnel files cannot be located. The number of ex-employees impacted is still being calculated but is believed to be in the region of 300-400.

33 As reported, Post Office made a disclosure to the ICO of this breach. The ICO has now asked a series of supplementary questions to which we must respond by 30th April 2020.

34 Given the nature of this incident it is possible Post Office will face regulatory sanction. Compliance is co-operating with the regulator. Our response to the loss of files and the changes to processes that have been implemented quickly will be taken into consideration. The support package that Post Office will to offer to those impacted, such as identity theft insurance and credit reference checking, also will be taken into account by the ICO when considering any action or sanction.

Belfast Data Centre Exit and move to the Cloud

35 IT Strategy is to exit the Belfast Data Centre in 2021 and move Horizon to a cloud based solution. IT have selected AWS as the partner of choice and contract negotiations will commence over the next two weeks.

36 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.

37 Many of the upstream contracts have restrictions in place for transfers of data outside of the UK or the EEA, and some for the use of Cloud-hosting services. Prior to any data transitioning all impacted contracts will have to be identified, the risk quantified and amendments negotiated. To achieve the timeframe of moving mid-2021 the Project will need to commit resource funding to support this workstream.

38 There is a risk that some clients will be opposed to this move and may not give their consent. Compliance is working with Legal and IT to assess those clients that we believe may resist such a move. We will be work with those clients, offering support and limited involvement with discussions. However, difficult decisions may have to be made where we are unable to secure consent.

39 There are aggressive timeframes in place, which will be challenging, though Compliance believes that the initial Contract negotiation deadlines can be achieved.

Financial Crime

Compliance with Money Laundering Regulations

40 109 new Bureau de Change cases were identified between 20th February and 19th April 2020 (up 18.5% from the same period in 2019). Case volumes through March and April mostly relate to currency buy-backs and multiple, small value purchases. However, the caseload has not yet shown any signs of decline as the Covid-19 crisis continues.

41 A new Bureau monitoring report was introduced in January, helping to identify branches processing multiple transactions just below the threshold for ID. This has helped us to take action in 3 branches to help prevent recurrence.

POL00423569

42 MI collated over the last two years shows controls have improved and new, significant non-conformance is stabilising. This is a result of improved monitoring since the implementation of AML Credence, which enables earlier detection and deployment of disruption/prevention activity.

43 The manual workaround to the Sanctions issue in AML Credence has been effective to date. The DCoE team and Accenture have progressed development of the solution and the estimated delivery date is during May.

Anti-Bribery and Corruption ("ABC") update

44 The new reporting and approval portal is in the final testing phases, with delivery during April. The improved workflows and reporting will help reporters and approvers ensure that requests are complying with Post Office policy and should improve conformance.

Whistleblowing Update

45 Post Office has signed a new contract with Navex Global Ltd for hosting the external whistleblowing speak up reporting channels. We are currently in the process of migrating onto the new platform, which includes a more structured information capture from reporters helping to improve investigations. The employee reporting channels are live and a One Update has been sent to all employees. Further communications to raise awareness are planned.

46 There has been an increase in reports during March including allegations relating to similar issues from two separate Supply Chain sites (please refer to the Whistleblowing MI in the Reading Room).

47 As a result of Covid-19, two branch related investigations have been put on hold, pending ability of assigned investigators to visit or speak to branches.

Fit & Proper update

48 A request was made to HMRC for the suspension of agent data submission for April due to resource issues, and we have also advised that we may be unable to comply with our own policy to obtain an annual F&P declaration from all our agents this year. HMRC agreed to the data suspension and asked that Post Office continues to monitor agents and take action if we deem any agent to not be F&P (e.g. through transaction monitoring or the Area Managers, Branch Analysis, Audit or Contracts teams identifying a concern).

49 We are requesting a further suspension for May, given the resource to resolve data gaps has been redeployed to support branches and outbound contact to branches is difficult in the current environment.

50 Additionally, the product team is looking to de-register a large number of branches to reduce costs. In recognition of this and the financial challenge Post Office is facing as a result of the Covid-19 crisis Compliance, together with Government Affairs, requested, through contacts in HMT, BEIS and HMRC that HMRC either allows Post Office to delay or reduce the annual registration charge payable in June 2020.

- HMRC has now advised that the annual fee can be deferred until 1st December 2020, which will allow more time for Post Office to assess on-going Covid-19 impacts and ensure we only register commercially viable branches for Travel Money. This will help manage cash flow and reduce costs.

51 Accenture is continuing with the design and build of the F&P system solution, with implementation expected June 2020. Funding for the project has been reviewed due to

POL00423569

the impact of Covid-19 and integration with Branch Hub is still being explored. However, this can be integrated with the front end at a later stage and should not delay delivery. The manual re-declaration process, which was planned for a small cohort of agents in May, prior to the delivery of the new system, is not going ahead to enable Postmasters to focus on continuing to provide services during these challenging times.

External Threats

52 The National Economic Crime Centre with support from UK Finance, has established a Covid Fusion Cell which meets a few times per week. It includes banks, Post Office, UKF, CIFAS, Insurance, IFB and British Telecom plus the public sector (NECC, HMRC, COLP, MPS) and shares information to help identify changes in the economic crime threat and criminal behaviour during the current restrictions. It targets where action can be taken to tackle criminal behaviour and provides alerts/typologies/comms to be issued cross-sector to help prevent economic crime.

- A response to an urgent section 7 request for intelligence from the Joint Money Laundering Intelligence Taskforce was provided by Compliance. This related to an individual implicated in a Covid-19 fraud attack on a major London hospital concerning the provision of urgent medical supplies for a major London hospital.

53 Suspicious banking cash deposits have continued throughout Covid-19, with a number of information requests received from the National Economic Crime Centre in relation to Project Admiralty. More suspicious banking cash deposits and bureau transactions are being identified as genuine transaction levels have reduced.

54 Further regulatory scrutiny for the gambling industry with Betway receiving a record £11.6M penalty for failing to verify the source of funds of customers and failing to effectively interact with a customer who deposited and lost £187K in two days.

- As a result of a lack of consideration of individual customers' affordability and source of funds checks, the operator allowed £5.8M to flow through the business, which was found, or could have reasonably been suspected to be, the proceeds of crime.
- Post Office provision of the Lottery has been previously assessed as low risk. Payzone services have yet to be assessed but we are aware it provides services for some companies that issue gambling credits, which may be higher risk.

Supply Chain Compliance

55 One assessment visit was undertaken during March, although this was reduced due to Covid-19 issues. Two "Improvement Needs" were identified, and an audit score of 6 was given, which is the average for Supply Chain.

56 No further assessment visits are taking place during this crisis period. However, twice-weekly communications are being issued to sites to help maintain compliance.

57 Guidance and process design support has been provided in respect of Covid-19 workarounds

- Loomis (Outward Branch ATM), RBS (Inbound processing from branches) and DWP (customer payments) to ensure contingency processes are compliant and robust.

Financial Services

Compliance Monitoring

POL00423569

58 Mystery shopping was paused on 17th March for social distancing and employee/Postmaster and contractor protection reasons. Further, branch FS activity has been significantly reduced, mostly following the cessation of Travel Insurance sales, suspending proposed savings and loans pilots and pausing the introductory activity with Capital One.

59 For the residual branch activity undertaken we have agreed a residual monitoring plan based on key risk indicators such as complaints and cancellations and continue to have regular 'check ins' with our Principals. The normal monthly compliance governance remains in place with our Principals albeit with a reduced level of MI.

60 Prior to lockdown we had been working closely with the Network on how we can secure and embed improvements to compliance and had made promising progress. Any re-start of network FS sales will need to ensure that branch colleagues and Postmasters have their product and conduct knowledge refreshed.

Results prior to 17th March 2020

61 CRM video mystery shops of BoI products remained Green;

- 28 mystery shops were undertaken and only one was red.

62 The risk rating for non-video mystery shops also remained Green

- From 101 counter shops completed there was only 1 red-rated savings shop. 96.8% of responses by mystery shoppers confirmed that they understood the information provided to them and that their understanding was checked by the clerk.

63 Travel Insurance mystery shopping was not within tolerance;

- 28% reds from 102 mystery shops – mostly due to issues with pre-existing medical conditions questions. This has been designed out for the re-launch that was due in April 2020.

64 Over 50s Insurance fared slightly better scoring 8% reds from 24 shops.

- The cause for Over 50s tended to be not checking customers had read the policy summary, which is an important requirement of the sale.

Training modules on Horizon and Success Factors

65 Recognising the strains on branches at this time we have been working with all stakeholders and the L&D team to ensure that we can provide some flexibility to the timetabling of completing the various training modules.

66 We have initially agreed to give an extension to the timetabling of the home phone and Broadband module to 7th July from 14th April and are agreeing extensions to the other modules due in the coming months, it is expected that by the autumn we would return to BAU timetabling, but will keep this under review.

67 The key message for everyone is that these modules remain crucial to training compliance and supporting customers and are crucial to demonstrating our commitments to stakeholders including regulators, business partners and Principals. The modules should be taken as soon as practicable, but there is greater time if this is needed.

Regulatory updates

68 The FCA provided guidance to firms on what, under its Principles for Businesses, they need to do to ensure that vulnerable customers are treated fairly and consistently across the

POL00423569

financial services sector. The draft guidance focuses on four key areas that firms should consider in their own approach to vulnerability:

- Understanding vulnerability
- The skills and capability of staff
- Taking practical action (through product and service design, communications, customer service)
- Monitoring and evaluation.

69 Firms should consider how they can meet vulnerable customer needs, e.g. a section in the app where a customer could disclose their personal circumstances and their needs, or the ability to add a designated second contact.

Mails – Dangerous Goods

Performance update

70 For P12, overall performance has dropped to 46% (made up of Inland 40% and International 73%). The main reason for failure is branches failing to ask clarifying questions and put on the appropriate label where required (following the Horizon prompts).

71 We have seen a decline in results since it was decided to start testing the scenario using a mobile phone with (but not connected to) a device a lot more. This scenario was increased as it was identified that branches were poor at conforming to the process. In reality, not many phones now have a separate battery which does present a challenge.

Actions underway to address performance:

72 Branch colleagues undertake an annual compliance module and test on Horizon for Dangerous Goods. Failure to pass prevents the colleague from transacting Mails. We have agreed with Royal Mail & the CAA to bring this module forward, which will go live on 12th June 2020.

73 As we are now adjusting to the 'new normal'. Area Managers will be discussing adherence to Regulatory Compliance across all areas with branches when they are making their calls. They will also be continuing to discuss the importance of using the correct mails conversation with every customer, every time. For the time being mystery shopping activity has been suspended by Ipsos, but the team will continue to discuss historic performance trends using the Branch Insight Tool. The Area Managers will also share a video with branches digitally to refresh colleague understanding of the correct transactional process.

74 We continue to monitor the Voice of Customer survey, to establish if customers were asked what was in their parcel. This information can be viewed by Postmasters and Area Managers in real time, with appropriate action taken. Year to date, the data confirms that this question is asked 75% of the time.

75 Once BAU visits commence again, Area Managers will continue to validate segregation of mail, checking for correct pricing and with actions agreed and recorded where appropriate; as well as continuing to coach colleagues on the process and use the Branch Insight Tool.

76 The Network team has initiated a piece of work to understand how we can improve the Dangerous Goods process on Horizon by asking the customer to complete a validation check using the Pin Pad. This will have a positive impact on adherence to the required process.

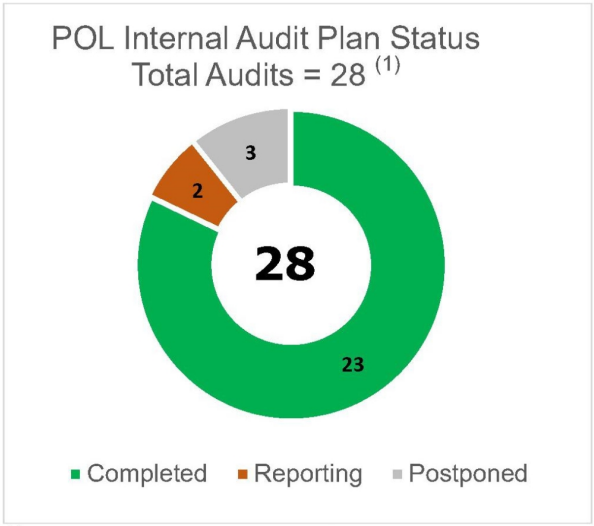
POL00423569

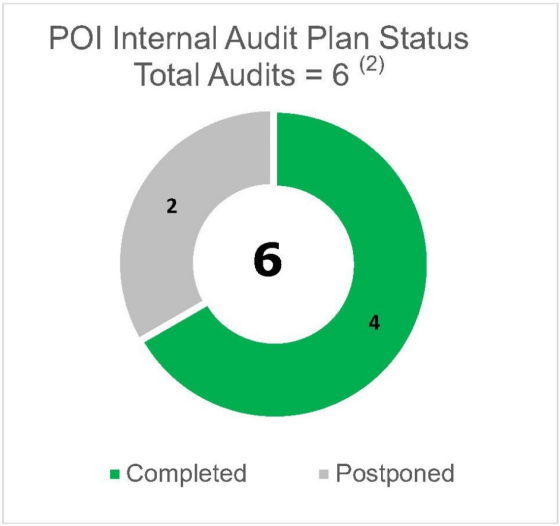
Internal Audit

Progress against 2019/20 plan

77 Completion of the 2019/20 internal audit programme progressed well, however, the final five reviews (three in POL and two in POI) were postponed in response to Covid-19 and reprioritisation of the Change Portfolio. Five audits were completed since the March ARC meeting, with the last two reports still being cleared with management at the time of writing this paper.

78 Current delivery status is as follows:





(1)POL ARC approved baseline plan for 2019/20 (18 core internal control reviews & 10 change assurance reviews). Details of the audit plan status are included in the reading room (Appendix 10).

(2)POI ARC approved baseline plan for 2019/20 (5 internal control reviews & 1 change assurance review).

Progress against 2020/21 plan

79 Following the March ARC meeting, we have developed a re-prioritised Internal Audit programme in response to the COVID-19 crisis. See separate paper submitted to RCC.

80 The following reviews from the revised 2020/21 Internal Audit programme are in progress or being planned for delivery in Q1:

Post Office Ltd			
	Review	**Status**	**Timing**
1	COVID-19 Programme Assurance	Fieldwork	20/04 - tbd
2	Maintain Minimum Control Standards	Fieldwork	20/04 – 29/05
3	Cyber Security Maturity	Planning	11/05 – 12/06
4	Health & Safety response to COVID-19	Planning	May
5	Effectiveness of Second Line during COVID-19	Planning	May
Post Office Insurance			
6	Data: Governance, ethics, privacy & security	Planning	May
7	Cyber Security (POL-POI Gap Analysis)	Planning	May
8	Incident and Breach Management	Planning	June

Confidential

POL00423569

3

Internal Audit reviews completed

81 COVID-19 priorities have delayed audit fieldwork and clearance of audit reports during March and April. Although we have completed five reviews since the March ARC meeting, two reports were still in final draft stage at the time of writing this paper. Details and latest status of these audits are as follows:

1	Postmaster On-boarding (Final)	
2	Vetting and Fit & Proper (Final)	
3	Change Control Framework (Final)	

4	Savings Accounts (Final Draft)	
5	FS Branch Sales (Final Draft)	

82 Our findings and observations from the three final reports are summarised below, with the full reports available in the reading room (appendices 11-13).

1. **Postmaster On-boarding** (Ref. 2019/20-23)



Sponsor:
Amanda Jones

Audit actions:

P1	0
P2	3
P3	1
Total	4

Appendix 11

Post Office has an obligation to Government to operate a minimum of 11,500 branches across the UK. This requires a pipeline of new Postmasters to take on new branches or take over existing ones. The churn rate is approximately 100 branches per month.

We conclude that the Postmaster on-boarding process is effective and confirm that the recommendations from the GLO working group have been incorporated in the new process. The responsibility and structure for delivering the on-boarding process changed in April 2019 when the function was restructured. The Postmaster on-boarding function, controls and processes have been re-organised and structured in such a way as to make the journey for a new Postmaster a more personal and less difficult experience.

The required level of control has been maintained through process changes to accommodate the single point of contact principle throughout the journey. The electronic business plan has been simplified and the interview process was improved. The pace of adoption of the new system and its ways of working has been good and continues to be maintained with all teams now working remotely for the duration of the Government lock-down.

Management Comment provided by Pam Heap (Head of Network Operations)

"A significant amount of work has gone into the improvements achieved this year to amalgamate what was 5 teams into 1 much smaller and more effective team to give the new incoming Postmasters a much more personal and trouble free on boarding journey.

With the challenges of new ways of working, cross functional training and introduction of a new CRM system and its related processes, I am both delighted with the results from the audit and very proud of all the hard work, resilience and commitment of the Bolton On boarding team."

POL00423569

2. **Vetting and Fit & Proper** (Ref. 2019/20-22)	
 ***Sponsor:*** *Al Cameron* *(Julie Thomas)* Audit actions: P1 0 P2 6 P3 3 Total 9 *Appendix 12*	The objective of this audit was to assess the design and operating effectiveness of the key controls around POL's Vetting and Fit & Proper processes. The audit found that Post Office have demonstrated a clear appetite and intention to operate effective Vetting and Fit & Proper processes to ensure that the right people are carrying out work on its behalf. However, policies and processes in place have suffered from a lack of clear ownership, exacerbated by ongoing organisational changes over recent years. **Vetting** We found that current vetting processes ensure that, at a minimum, criminal and financial checks are carried out for all employees, contractors and agents, and we confirmed that enhanced controls are in place to cover Supply Chain staff. However, vetting activities are fragmented across the business, with varying levels of guidance, outdated policies and no clear overall ownership. Additionally, checks on professional qualifications are not carried out as a matter of course and there is no process for re-vetting outside of Fit & Proper and Supply Chain. **Fit & Proper** The Fit & Proper Policy was detailed and up-to-date and significant work has been undertaken to identify affected direct employees, agents and commercial partners. A clear record of current compliance was in place as of November 2019, with action taken to de-register non-responding or unsuitable partners. However, we noted that current practice is not fully aligned to the Fit & Proper Policy, as ongoing identification and management of direct employee 'responsible persons' sits with Compliance rather than HR. This increases the risk that changes in personnel are not identified in a timely manner.

Management Comment

"I believe this report reflects accurately the current position with Vetting and Fit & Proper policies and processes. Whilst the responsibilities are split across HR and Operations functions, I have agreed to take the lead on behalf of Post Office as the majority of vetting is for the c.50,000 assistants. Additionally, as we move to a fully franchised organisation, the ownership of Postmaster Contracts, including their conformance and compliance obligations sits within Operations. A new Head of Contracts will be appointed and, along with Postmaster contracts and policies, ownership of the Vetting and Fit & Proper Policies will be added to their role. This decision has been taken in agreement with Lisa Cherry, Group HR Director."

Julie Thomas – Operations Director, Network Operations

"I can confirm that I believe this is a fair assessment of the Fit & Proper and Vetting status in the business. We will continue to provide compliance assurance oversight of the processes and outcomes and our capacity challenge will be closed when our new Policy and F&P compliance manager joins the team shortly."

Jonathan Hill – Director of Compliance

Confidential

POL00423569

3. **Change Control Framework (Operating Effectiveness)** (Ref. 2019/20-24)	
 Needs Improvement ***Sponsor:*** *Dan Zinner* Audit actions: P1: 0 P2: 2 P3: 3 Total: 5 *Appendix 13*	Between July and August 2019 Internal Audit completed three design effectiveness reviews over specific areas of the change process, i.e. gating, benefit realisation and second line assurance activities, noting some areas for improvement. A key observation was the need to formalise a control framework for change activities with a clearly defined set of responsibilities. The objective of this follow-up review was to assess to what extent the previous audit recommendations have been implemented and operationalised. We concluded that Post Office have made significant progress in designing and implementing a Change Control framework which is helping to guide actions through identifying control failures and creating remediation plans. It is acknowledged by SPO that the framework is not yet operating as intended, as shown by SPO's own self-assessment. Work continues to refine the framework and to embed control delivery and monitoring. While the current level of control effectiveness may be perceived as low, we consider it to be in line with the expected level of maturity at this early stage of implementation and highlight the good progress that has been made. We also note SPO's commitment to improving performance and raising maturity to a good standard. The report highlights further areas of improvement that would elevate the framework's maturity.
Management Comment provided by Dan Zinner (Group Chief Strategy & Transformation Officer) "I have read the report and applaud the SPO team for creating the necessary CCF, which is in the process of being embedded. Any framework can be improved upon and I would appreciate IA's ability to highlight high risk areas where more control is needed, to ensure there is a balance between investment in increased controls and the investment needed to improve the resources knowledge, understanding and behaviours on how to do the right things, to prevent the root cause of control flags."	

Status of Audit Actions

83 Audit actions are generally being completed on time. The movement and ageing of audit actions are shown in the table below (status at 29 April 2020).

Audit Action Status (POL):	
Open actions at last ARC	64
Less: Actions closed in period	45
Add: New actions in period	33
Total open actions	**52**

Ageing:	
Open (not yet due)	52
Overdue (<60 days)	0
Overdue (>60 days)	0
Total open actions	**52**

84 There were no overdue actions at the time of writing this report, however, five actions were due on 30 April 2020. We highlight that the change to business priorities may cause delays in completion of these actions and we will work with the action owners and GE sponsors to identify actions where it is appropriate to grant extension to the agreed completion dates.

POL00423569

3

Appendix[2]

Central Risk

Appendix 1: Non-COVID-19 enterprise & intermediate risks
Appendix 2: COVID-19 risk data set
Appendix 3: Change Portfolio

Compliance

Appendix 4: Whistleblowing MI
Appendix 5: Summary Compliance Dashboard
Appendix 6: Compliance Dashboard
Appendix 7: Covid-19 Regulatory Dashboard
Appendix 8: Telecoms Regulatory Calendar
Appendix 9: FS Regulatory Calendar

Internal Audit

Appendix 10: Internal Audit Plan (2019/20)
Appendix 11: Internal Audit Report – Postmaster On-boarding
Appendix 12: Internal Audit Report – Vetting and Fit & Proper
Appendix 13: Internal Audit Report – Change Control Framework

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

Confidential

POL00423569

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

4

Title:	2020/21 Internal Audit Plan	**Meeting Date:**	6 May 2020
Author:	Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer

Input Sought: Noting / Discussion

The committee is asked to:

- note the internal audit priorities during the COVID-19 crisis;
- consider if the proposed reviews and activities are appropriate to support management during the crisis, whilst continuing to provide assurance to the Audit, Risk & Compliance Committee (ARC) over key risks to Post Office;
- advise on other risks or business areas that Internal Audit should consider in the short and medium term.

Previous Governance Oversight

Feedback from the March ARC was that the proposed audit programme for 2020/21 was no longer appropriate in light of COVID-19 and should be restated to focus on immediate priorities that will support the business during the crisis.

Executive Summary

The 2020/21 Internal Audit plan was re-assessed alongside new risks emerging from the COVID-19 pandemic and Post Office's response to manage the business through the crisis. This paper presents the priority activities and reviews that Internal Audit will focus on in the short term.

Confidential

POL00423569

Questions addressed

1. What processes, activities and programmes from the 2020/21 Internal Audit programme should be prioritised during the COVID-19 crisis?

4

Report

Introduction

2. Post Office objectives during the COVID-19 crisis are:
   - Protecting our whole workforce;
   - Keeping the Branch Network operating and open for business;
   - Looking after our elderly, vulnerable and at risk customers;
   - Ensuring our supply chain remains stable and secure;
   - Maintaining communications with our colleagues, postmasters and customers; and
   - Emerge from the crisis with a plan for a fast start.
3. To support these objectives, Internal Audit's role must adapt to provide value to Post Office beyond our typical remit. Non-audit activities may include supporting the business in its short-term response to the crisis and long-term recovery efforts. Audit activities will focus on processes or change programmes that have become critical in the response to COVID-19 and/or have seen an increased risk as a result of the crisis.
4. We have already adapted our ways of working to maintain productivity while working remotely in an all-virtual environment. This includes the increased use of 'agile auditing' and more flexible working arrangements to balance work and family obligations.

Approach to the re-prioritised Internal Audit plan

5. We have shifted to a dynamic audit programme that will be reactive to emerging risks and management requests for support. The audit programme will be reviewed and refreshed at every RCC and ARC to ensure it remains relevant and appropriate.
6. With the help of the Risk team, we have assessed risks arising from COVID-19 around people, network resilience (including IT DR) and Supply Chain. We consider the current management interventions and mitigations to be appropriate and not requiring assurance by Internal Audit as a priority. We will maintain a watching brief on these areas.
7. We have also assessed the potential consequences of COVID-19 on the general control environment to identify the short and medium term priority areas where Internal Audit should focus – these are priority areas from the 2020/21 audit plan as well as topics identified in response to COVID-19.
8. The remaining topics from the 2020/21 plan have been placed on a watch-list for ongoing review and will form the basis of the audit programme when we resume normal operations.

Revised Internal Audit plan

9. Table 1 below shows the top five internal audit priorities. The rationale and high level scope is included in appendix 1:

POL00423569

Table 1: Top 5 priorities			
	Review / Activity	GE Sponsor(s)	Timing
1	COVID-19 Programme Assurance / Support	Nick Read	Ongoing
2	Maintain Minimum Control Standards	Al Cameron	Ongoing
3	Cyber Security Maturity	Jeff Smyth	May
4	Health & Safety response to COVID-19 crisis	Al Cameron	May
5	Effectiveness of Second Line during COVID-19	Al Cameron / Ben Foat / Jeff Smyth	Ongoing

10. Table 2 represents additional areas for review, which are not immediate priorities, but important to do as soon as possible.

Table 2: Medium priority reviews			
	Proposed Review	GE Sponsor	Timing
1	GLO Operations Improvement Programme	Al Cameron	Sept
2	Postmaster Reporting (MI, Branch Trading Statements)	Amanda Jones	Q3
3	BCP Post-crisis assessment	Jeff Smyth	tbc
4	Branch Hub	Al Cameron	Q4
5	Stamp Stock	Al Cameron	Q4

11. Table 3 is our 'watch list' and includes all of the areas that are not included in the immediate and medium term priorities. This will form the basis of the Internal Audit plan when normal operations resume.

Table 3: Watch list		
Core Processes / Risk Based Reviews		Core / Risk
1	Branch Cash Forecasting	Core
2	Financial Controls Framework	Core
3	Mails & Parcels	Core
4	Travel Money	Core
5	Business Continuity	Core
6	IT Operations	Core
7	Fixed Assets	Core
8	Treasury Operations	Core
9	Product Risk Assessment (MoneyGram)	Core
10	Identity and Access Management (JML)	Risk
11	IT DR	Risk
12	Digital Strategy	Risk

Confidential

POL00423569

13	Effectiveness of Financial Crime Function	Risk
14	Contract Management	Risk
15	Effectiveness of Risk Management Framework	Risk
16	Agent Remuneration (3rd Party Data)	Risk
17	Compliance with Prompt Payment Regulations	Risk
Change Assurance Reviews		Governance / Programme
17	PCI Compliance Programme	Programme
18	Belfast Exit / Cloud Enablement	Programme
19	Change Controls Effectiveness	Governance
20	Resource Management (for Change)	Governance
21	Arrow/Data Platform – follow-up	Programme

Post Office Insurance Internal Audit Plan

12. The steer from the POI ARC was to work with management to identify which internal audits will be most helpful to support POI during the COVID-19 crisis. Following discussions with management and POI RCC on 28 April 2020, the following priorities have been identified:

	Process / Area	Priority
1	Data: Governance, ethics, privacy and security	High
2	Cyber Security (POL-POI Gap Analysis)	High
3	Incident and Breach Management	High
4	Channel review: Non-branch sales	Medium
5	Effectiveness of Risk Management	Medium
6	Pricing: Principles, policies and process	Low
	Alternative topics (Watch list)	
1	MI Platform	
2	Revenue Recognition	
3	Capital & liquidity management	
4	Marketing and financial promotions	
5	Strategy planning and tracking	
6	IDD follow-up	

Confidential

POL00423569

Appendix 1 - High level audit scope statements

Rank	Review	Rationale for inclusion and high level scope
1	COVID-19 Programme Support / Assurance	The COVID-19 Programme is critical in coordinating and managing Post Office's response to the crisis. It is also central to managing the risks emerging from, and relating to, the pandemic. Internal Audit will seek to be engaged in the programme as a critical friend as well as in more hands-on capacity if required (e.g. to shadow the PMO). We will offer to challenge and validate criteria and MI used to drive business critical decisions. We will use the information obtained from the programme to respond pro-actively to emerging risks and reactively adjust our approach to other audit activities. The scope will include an assessment of Post Office's response to COVID-19 related risks, for example people risk and H&S.
2	Maintain Minimum Control Standards (Financial, IT and Operational)	In order to ensure ongoing operations, it is likely that normal controls may be relaxed or compromised through temporary work-arounds, home working, staff sickness, etc. Internal Audit will consider the impact of these measures on the continued operation of key controls to ensure the minimum control standards are being followed to operate safely and to prevent fraud. We will provide a layer of oversight where the normal management oversight and second line assurance activities may be reduced. This will include an assessment of segregation of duties adjustments, measures in place to approve via substitutes, exception management and tracking of relaxed controls. We will link closely with output from COVID-19 steerco. Starting with controls over cash, we will perform a number of short focused reviews to determine to what extent the normal control frameworks / standards have been relaxed and then do more targeted reviews proportionate to the risk.
3	Cyber Security Maturity	There is a heightened cyber security risk during the COVID-19 crisis as evident by increased volume of attacks. The risk is further increased by all-virtual working, newly adopted functionality / work-arounds to support home working, increased mobile device usage, etc. This audit will assess the implementation of the agreed actions and evaluate the level of progress towards increased Cyber Security Maturity following the 2019 Deloitte assessment. Progress will be assessed across the highest risk domains and those areas highlighted by the 2019 review to be in most need of improvement. The scope will include areas of increased risk as a result of COVID-19, for example mobile devices and relevant elements of JML (access management). It will also cover the risk exception / acceptance process for any controls that may be relaxed during the crisis.
4	Health & Safety response to COVID-19 crisis	Post Office employees, branch staff and customers are exposed to H&S risks directly from COVID-19 and indirectly from the operational response to the crisis. This review will assess the effectiveness of Post Office's response to mitigate these risk. The scope will include (but not limited to): Mechanisms introduced to monitor H&S risks and MI driving key decisions; response in business critical areas such as Supply Chain; PPE procurement and guidance; effective communication with employees, postmasters and customers; liaison with Unions /NFSP and tracking their concerns; tracking of COVID related incidents / concerns logged with management; initiatives to combat mental health impact and impact of prolonged home working on colleagues; follow-up of findings from recent external H&S audits that may worsen due to focus on COVID response; and, tracking the backlog of BAU H&S tasks that have been put on hold whilst managing the pandemic.

Confidential

POL00423569

5	Effectiveness of Second Line during COVID-19 crisis	Changing operational requirements and pressures during the COVID-19 crisis may divert resources away from the second line, resulting in the distinction between first and second line activities being less clear. This may be exacerbated by staff sickness and virtual working. Internal Audit will perform short, focused reviews of key second line assurance activities (Risk, Compliance, Financial Controls, IT Controls, IT Security, etc.) to assess if they continue to operate effectively amid the crisis. We will flag any decline in the operation of the second line and may support the business by providing interim assurance over affected areas until the second line can resume full operation.
Medium Priorities		
6	GLO Operations Improvement Programme	As a result of the Group Litigation Order outcome and settlement (Q4 2019) Post Office created a Post GLO programme to address the findings and recommendations set out in the Common Issues Judgment and the Horizon Issues Judgment. This is a joint programme between Legal and Operations, each with its own workstreams. Post Office's response to the GLO findings will continue to attract scrutiny. Internal Audit will assess overall programme set-up and governance and also review specific workstreams (most likely those working on improving front-office and back-office operations for the benefit of postmasters.)
7	Postmaster Reporting (MI, Branch Trading Statements)	Providing Postmasters with fit-for-purpose information and communication was identified by the GLO as an area that requires improvement. Access to timely, accurate and useful information has become even more important during the COVID-19 crisis. The objective of this audit is to assess the design and operating effectiveness of the mechanisms and processes to provide timely, accurate and reliable MI to postmasters. This may include a review of the systems and MI that are being developed to generate and facilitate reporting to Postmasters.
8	BCP Post-crisis assessment	Once the organisation has stabilised from the initial crisis, there will be an opportunity to record lessons learnt from the experience, which will be valuable for future business interruptions. There may also be a need to adjust the standard BC plan to reflect the 'new normal', which brings its own risks and challenges. Our review will assess the lessons learnt exercise performed by the business, or facilitate such an exercise if required.
9	Branch Hub (Programme Assurance)	The Branch Hub programme is working at pace to deliver functionality that will support the Operations Teams during the COVID-19 crisis and alleviate pressure on the Branch Service Centre. Internal Audit will assess the governance and delivery of the programme, in particular controls assessed as weak in previous audit reports and those controls that may be compromised when working to such demanding timelines (e.g. clarity of requirements, change control, decision gates, risk management, testing).
10	Stamp Stock	Management request to review the controls over stamp stock. System functionality for recording and reconciling inbound and outbound stock remittances is currently limited and stock returns are not validated (counted) in full. The objective of this review is to ensure that the risk of incorrect stock adjustments, which may be to the detriment of Postmasters, is minimised and that stock control measures are in place to minimise theft and financial crime.

Confidential

POL00423569

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

Title:	PCI – DSS Programme Update	**Meeting Date:**	06th May 2020
Author:	Joseph Moussalli, Programme Manager PCI DSS Programme	**Sponsor:**	Jeff Smyth, Group Chief Information Officer

5

Input Sought: Noting

RCC is requested to note programme progress in the last reporting period.

Previous Governance Oversight

- Programme progress since the last ARC update on 24th March 2020.

Executive Summary

Status of the programme
The programme is expecting to obtain Ingenico final banking software deliverables in early February 2021 and to commence branch rollout in late March 2021. Branch rollout will be completed in May 2021 and formal PCI-DSS accreditation will be achieved by June 2021.

Covid-19 - there is no significant impact to the overall programme critical path delivery timeline at this stage.

The main achievements / status since the last ARC update are listed below.

Business Case - £15.8m has been approved at PRB. The business case will be presented at IC and the Board in late May 2020.

Integrated Programme Plan - Planning sessions were held with all suppliers. Further work is ongoing to see how the delivery plan timeline can be further improved.

Ingenico CEO to CEO Executive call
Ingenico & Post Office PCI DSS Executive Call (with Nick Read) was held on 16th April 2020.

Key points discussed:
- Ingenico development team is currently on schedule with both the EMV (Retail) and Banking deliverables.
- The contracts for "build" and "run" have been impacted by inclusion of Coronavirus addendums – and are now due June 2020 but the legal activity is not impacting technical delivery.
- The PED deployment has been paused due to Coronavirus. Discussions focused on ensuring a rapid re-start.

IT work stream
- Three delivery phases for the workstream identified.
- PED firmware rollout paused due to Covid-19.
- IT workstream development reported on track.
- Key milestone: Ingencio has delivered the C3 banking specification.

Confidential

POL00423569

Target Operating Model (TOM) work stream

- Eight TOM delivery releases identified. Three of these releases are dependent on the P2PE solution release.
- TOM work is currently tracking to plan however there is cost / timeline risk and therefore significant focus is being placed on this activity. Several TOM remediation items are still in analysis or design.

Questions addressed

1. What progress has been made since the last update in March?

2. What is the latest status of the commercial negotiations with Fujitsu/Ingenico?

3. What is the current timeline for regaining PCI DSS compliance?

4. What are the major activities due to complete in the next two month period?

Report

5. This paper explains the progress made by the PCI DSS programme covering all significant activities across the three core workstreams;

   - IT Workstream – to deliver Point-to-Point Encryption (P2PE) for standard Retail payments and banking transactions.
   - Target Operating Model (TOM) – to remediate products and all operating processes required to ensure internalised PCI-DSS compliance.
   - Branch/Client Communications (Comms) – client update sessions across Post Office's acquirers, banking framework and other partners.

6. The plan for regaining PCI DSS compliance has been substantially refined this month. The latest plans and supplier inputs indicate the solution will be ready for branch rollout commencing late Q1 2021. Branch rollout would be substantially complete providing compliant ready systems by Q2 2021 ready for the audit to complete. This timetable has not been formally communicated externally. It will be communicated once we gain more confidence that the key suppliers are consistently tracking to milestones.

IT Workstream Update

7. The integrated planning exercise with all parties has identified three delivery releases for the workstream:
   - Release 1: Retail Payment release (card payments) – technical Pilot for 5 counters in multi-counter branches.
   - Release 2: Banking capability introduced – all P2PE systems live ready for the branch rollout.
   - Release 3: Branch rollout of POS and PEDs.

POL00423569

Summary of key items delivered since the last report:

- PED firmware rollout – since the last report we have completed 74% (18,882 of 25,400 PEDs) of the rollout. Deployment paused on 25th March due to Covid-19. We have plans to resume the rollout on 1 July or sooner subject to lockdown restrictions being lifted.
- Retail Payments and banking transactions development reported on track by Ingenico.
- Vocalink test environment and connectivity to Ingenico development has been completed.
- Test POS has been delivered to Ingenico at Dalgety Bay for integration testing.
- TMS tool for chain of custody – diagnosed issue with duplicates. PED data now being re-loaded.

8. Commercial negotiations have progressed significantly across all suppliers required for delivery. The negotiations cover commercials for project implementation (build, test and deployment of the new solution), and ongoing Business As Usual (BAU) commercials relevant to running and maintaining the service once live. All parties have commenced work at their own risk as a goodwill gesture to ensure programme timelines are maintained and all delivery resources are now mobilised.

Pin pad upgrade:

9. We discussed the paused position of the field PED upgrade/deployment programme with Ingenico and agreed that we will now jointly revisit available options to reduce mobilisation timelines for when we restart this workstream. In headline terms, we will explore how we might engage a minimum "warm tick-over" resource team that would allow an accelerated re-mobilisation rather recommence from a "cold" standing start. We will assume that we are aiming for a 1st July 2020 restart (of course subject to safety considerations) and execute a joint work through of resourcing options to maximise knowledge retention and ramp-up capabilities. We'll provide an update at the next executive session but won't wait to take action if we agree tactical priorities.

Santander moving to the P2PE payment channel

10. Santander has confirmed that they understand the change required to support our P2PE solution by migrating transactions to flow through Vocalink. However, the proposal and timelines are on-hold pending the lifting of the Covid-19 lockdown restrictions.

POca moving to P2PE payment channel (JP Morgan)

11. Discussions have been held with JP Morgan about the solution. A proposal has been requested for a target date 15 May.

Fujitsu/Ingenico Banking and Payment Transaction Processing Commercials:

12. Project implementation "build" commercials are fully agreed with Fujitsu, the contracts have been signed by POL and are still progressing through a final Ingenico governance cycle. A late request was received from Ingenico to add some terms to cover the Covid-19 situation. There is pre-commitment in place for costs with delivery timelines confirmed and the delivery work is progressing.
13. BAU "Runtime" commercials for the payment and banking solution – the first draft of the BAU terms have been received from Ingenico by Fujitsu. These BAU financial heads of terms have been shared - work is in progress to complete contract drafting.

POL00423569

14. The two contracts were discussed at the executive meeting on 16th April. The progress of the "build" statement of work and the "runtime" MSA contractual documentation were due to be completed but they have been delayed by Coronavirus schedule reviews. It was recognised that it would take time to work through all parties and Ingenico have endeavoured to push internally for an improvement to the current target completion date of 30th June 2020. Everyone recognises that the legal review/finalisation is not impeding technical progress but equally everyone agreed it would be useful to get the task completed.

Vocalink Commercials:

15. Legal and procurement teams have provided feedback and identified areas where the existing Vocalink contract is not sufficiently robust to support the work. The Post Office and Vocalink legal teams need to review the proposed amendments together. However, Vocalink legal team availability is limited. Contract amendments are forecast to be completed by the end of May 2020. Delivery activities are proceeding in parallel, so no time is being lost alongside commercial finalisation work.

Fujitsu / Ingenico Software development activities - to support Card Payments and Banking transaction processing. Activities include:

- Card Payments development
  - Fujitsu has completed the Design for to progress the development for the Global Payments Accreditation.
  - POS Test Counter in Dalgety Bay has been set-up and is now awaiting Ingenico verification.
  - Test cards have been provided
- Banking transactions development
  - Network connectivity between VocaLink and Ingenico to support critical path activities is in place pending Ingenico verification.
  - AXIS AH plug-in integration testing in progress.
  - Banking API Specification work has started.

16. Ingenico have been able to use emulators and Magstripe to progress the development whilst waiting for Bank cards from Vocalink. Due to Covid-19 MasterCard has placed a restriction on site visits so Vocalink have been unable to create the cards. This was escalated and the cards for the immediate acquirer hub development will be made available in good time for the Ingenico development.

17. Nevertheless the Coronavirus situation is acknowledged as very fluid and therefore we have agreed to jointly "workshop" various scenarios to understand future risk mitigation steps that may be required should the lock -down situation persist.

Confidential

POL00423569

Service Increment (SI):	Post Office (Banking Capability) Impact	SI Start Date:	SI Release Date:
SI-17	Detailed Planning (EPIC Creation)	29/Jan/20	22/Apr/20
SI-18	Development Start	25/Mar/20	17/Jun/20
SI-19	Further Development	20/May/20	12/Aug/20
SI-20		15/Jul/20	17/Oct/20
SI-21	Development Complete (Core Functionality)	09/Sep/20	02/Dec/20
SI-22	Development End	04/Nov/20	27/Jan/21

5

A request for an update on SI-17 has been requested.

Target Operating Model (TOM) Workstream Update

18. The PCI programme continues to progress activities to remediate non-compliant PCI-DSS processes and products. The plan for the TOM workstream has been substantially updated. Current analysis indicates all product and process remediations are not on the critical path for the programme. The Payments over the telephone solution is tracking 4 weeks late (now due early May 2020) but it is not expected to delay the overall programme.

19. Since March, the following activities have been completed:
- The TOM plan has been substantially updated and reviewed.
- High Level Design v1.1 has been approved by EAG in principle for those elements that are known and able to be progressed to the build phase.
- PAN obfuscation on screen and on receipts for products has been commissioned with ATOS.
- The design for the Obfuscation of PAN in the Fujitsu data centres has been completed.
- Eight TOM releases have been identified and three of these depend on the P2PE solution.
    - Release A: PAN on screen and receipt obfuscated
    - Release B: Telephone payments secured. CHD in Call recordings mitigated.
    - Release C: Obfuscation of CHD in Fujitsu data centres remediated.
    - Release D: Travel money card top-up process remediated.
    - Release E: Fujitsu back end reconciliation process adjusted.
    - Release F: Quatrix – process for CHD
    - Release G: Financial Service and Financial Crime team process adjusted.
    - Release H: Payment of Credit Card Bill Payment (Santander)

20. Key areas of the TOM workstream that are still in analysis or design are:
a. Telephone payments (proposal from Verizon is due early May)
b. Voice recordings – mitigation of calls with PAN data.
c. Financial Crime Team / Financial Service Centre team payment investigations. Discussions ongoing with Barclays about whether these investigation can take place using transaction details instead of card details.
d. Data network scanning – the remediation approach is being discussed with the Compliance team
e. Payment of Credit card bill (Santander)
f. Reconciliation design (post P2PE implementation)

POL00423569

A dashboard illustrating the scope, supplier involvement and timelines can be found in the appendix.

Branch/Client Communications (Comms) Update

21. Continued successful regular client update sessions have taken place with Global Payments and American Express, Post Office's acquirers, and Nettitude, Post Office's quality security assessor (QSA). Positive feedback was received from all parties. However, the latest delivery timeline has not been shared with the Post Office client base (e.g. banking, bill payments) until we have more certainty in the plan.

Major activities due to complete in the next two month period by 19 May 2020 (Status now)

- PED firmware upgrade to v6.04 to be completed (including deployment of POca PIN change functionality). On-hold due to Coronavirus 74% completed.
- Ingenico – Service Increment 17 (EPIC creation) completed – ready for development Service Increment 18 work commencing on 25th March 2020. Reported on track by Ingenico – further information on progress requested.
- Vocalink test environment stand-up and testing scheduled for 24th April 2020. Completed
- Planning of JPM and Santander cutovers to the new solution. Meetings held. Santander impacted by Covid-19. JPM proposal targeted for 15 May.
- TOM – HLD approved. Baseline remediation plan. First tranche approved and planned. Second tranche still in analysis /design.
- First draft of end to end acceptance testing goals and plan (and successful exit criteria). End to end test strategy being drafted – meetings held with suppliers
- First draft of solution deployment options including parallel running reconciliation strategies and tooling needs. First draft available – discussions on-going.

Risk Assessment, Mitigations & Legal Implication

22. ***Risk:*** Risk of loss of confidence by our client base should a delay occur.

Mitigation: Pre-emptive conversations have already taken place with client-facing senior Post Office stakeholders to formulate a strategy should a delay need to be communicated. The strategy could be to break down the progress into phases and also to indicate how the progress has been affected by Covid-19.

23. ***Risk:*** Risk of the solution provider encountering complexities while developing the new solution as this is a new venture for them.

Mitigation: Post Office has requested Ingenico to provide granular level reporting to allow close monitoring of progress. Therefore, if there are any blockers encountered they can be discovered and addressed quickly.

Confidential

POL00423569

24. ***Risk:*** Risk of Coronavirus impacting the pin pad refresh project (as this activity has direct branch access dependencies); there is a chance that the activities will not be complete by the end of April as required by Post Office's acquirer and card schemes. This risk became an issue and the activity has been paused until the lockdown can be lifted -expected by 1 Jul 2020. This is not on the critical path for the programme.

    Mitigation: The risk has been discussed with Post Office's acquirer Global Payments. Global payments have confirmed that the PCI council has formally confirmed that the expiry of the PTSv3 software installed on the Post Office's pin pads has been extended by 12 months to April 2021. This risk is now adequately mitigated.

25. ***Risk:*** Risk of 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.

    Mitigation: Post Office has begun 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. In particular, we will be evolving the inter-organisational delivery model to anticipate greater levels of remote and collaborative working as we expect this will become the normal operational mode for the foreseeable future.

26. ***Risk:*** There is a risk to the programme timescales and costs that that post branch rollout clean-up activities may be needed on legacy data. This may include deleting legacy data, awaiting for it to be rolled-off or in certain cases putting PCI DSS controls in place. Known areas of risk include Audit SAN, Transaction Enquiry Service, CC audit log (INTrust), call recordings.

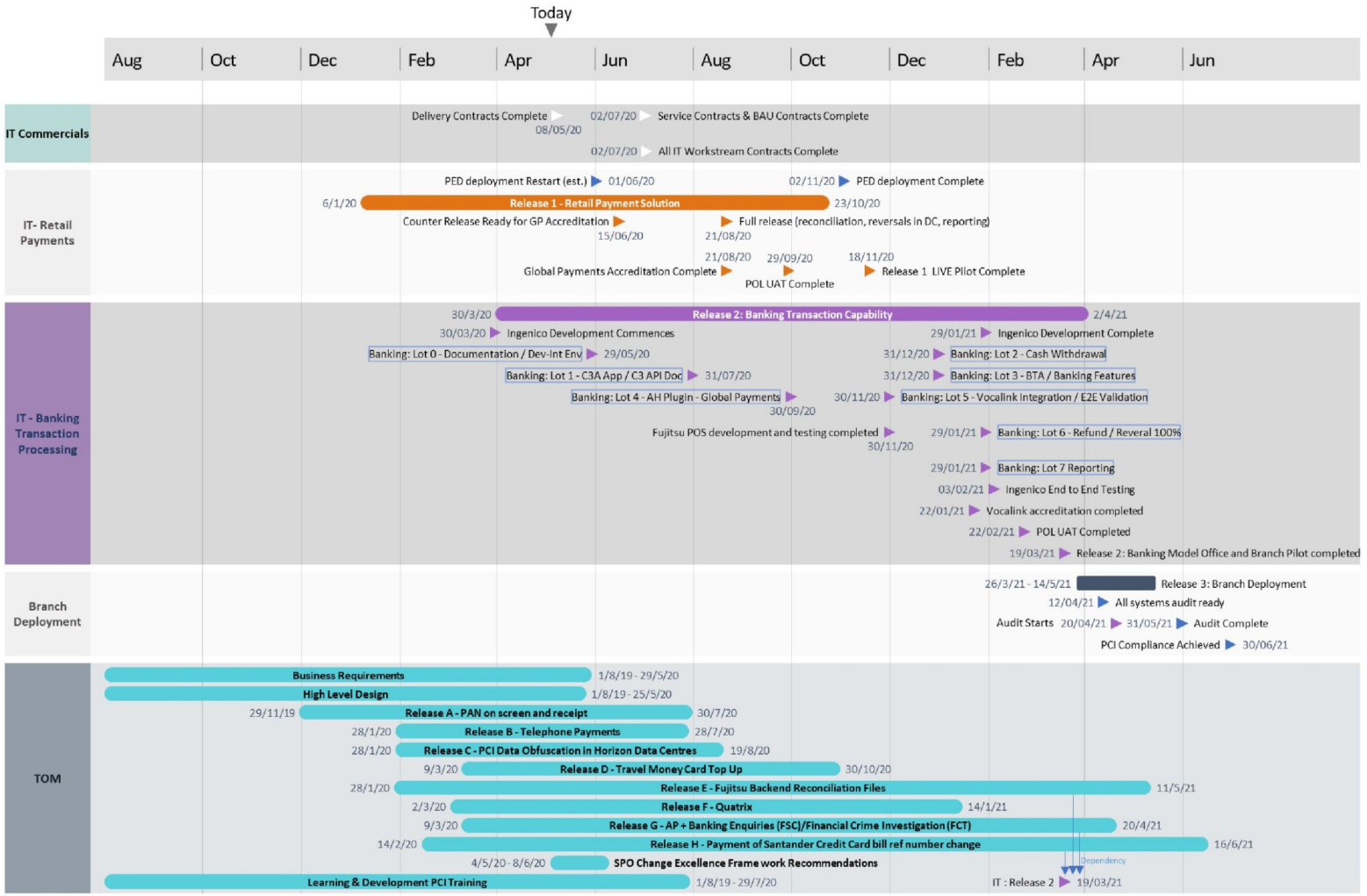
    Mitigation: Post Office is conducting further analysis with suppliers and compliance to mitigate the risk to the programme timescales and costs.

Stakeholder Implications

27. Post Office banking clients may use any extended timelines to regain PCI-DSS compliance as a mechanism to negotiate concessions on the present or forthcoming banking framework agreement. The regular client update session will provide them with a forum and information to help manage our key messages with their internal stakeholders. Further mitigation strategies may be required if we see a shift in their current position. The programme communication workstream will address that need should any specific arise.

POL00423569

Appendix - Programme plan



Confidential

POL00423569

Quarterly Audit: These regular audits maintain a level of visibility of our compliance with the QSA. These are also used to communicate our compliance status with our clients.

Appendix – TOM Dashboard

	Name	Complexity	End-to-End Delivery					
			Discovery	Design	Build	Test	Service Readiness	Deploy
Products	One4All Gift Cards	M	03/12/2019	23/03/2020	08/05/2020	29/05/2020	13/05/2020	22/06/2020
	Travel Money Multi Currency Card	M	03/12/2019	23/03/2020	**31/07/2020	**18/12/2020	**16/02/2021	**16/01/2021
	Pre-Paid Debit Cards	M	03/12/2019	23/03/2020	**31/07/2020	**18/12/2020	**16/02/2021	**16/01/2021
	Payment of Credit Card Bill (Santander only)	H	29/01/2020	10/04/2020	11/06/2020	03/07/2020	31/07/2020	07/08/2020
	Budget Card	L	03/12/2019	23/03/2020	08/05/2020	29/05/2020	13/05/2020	22/06/2020
Processes	Automated Payments Enquiries + Banking Enq	H	09/03/2020	27/03/2020	**31/07/2020	**18/12/2020	**16/02/2021	**29/01/2021
	Telephone Payments	M	29/01/2020	*27/03/2020	*29/06/2020	*20/07/2020	03/08/2020	11/08/2020
	Financial Crime Investigation	H	09/03/2020	27/03/2020	**31/07/2020	**18/12/2020	**16/02/2021	**29/01/2021
	Fujitsu Back End Reconciliation Files	H	11/03/2020	17/04/2020	15/05/2020	12/06/2020	09/06/2020	03/07/2020
	Email	L	31/03/2020	01/05/2020				
	File Data Storage	TBC	31/03/2020	01/05/2020				
	Quatrix	TBC	31/03/2020	01/05/2020				
	Mimecast	TBC	31/03/2020	01/05/2020				
	POL SAP Archive	TBC	31/03/2020	01/05/2020				
	Credence	TBC	31/03/2020	01/05/2020				

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

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

POL00423569

Communication plan – Internal

Meeting Name	Schedule	Frequency	Objective	Attendees
Executive Steering Committee	N/A	Monthly	CEO level conversation to maintain focus and momentum of delivery	Nick Read and Ingenico accountable executive
Steering Committee	N/A	Fortnightly	Inform stakeholder of progress Share any impact of change schedules Request guidance on significant decisions Ratify RAID items with their mitigations Escalate blockers and seek assistance to remove Capture and progress actions	Sponsor: Jeff Smyth IT: Rob Wilkins Business: Andrew Goddard (Payments) / Martin Kearsley (Banking) Finance representation: Alistair Roman Business Operations: Kim Abbott Corporate Risk: Rebecca Barker Corporate Communications: Lisa Mobley Information security: Tony Jowett Legal: Ken Garvey Fujitsu: Wendy Warham / Dan Walton Ingenico: Dave Allen Vocalink:Carl Aveyard
Internal IT Work stream Huddle	10:00	Daily	Internal forum- Work through current actions and create next actions, on 'Teams', tracking tasks to milestones and overall plan	James Foulk (PMO) Alex Wood (Solution Architect) Wayne Fitzgerald (PED Deployment PM) Oliver Sutherland (PMO) Sara Fouad (PM)
RAID, Milestone, Review	Thurs 14:30	Weekly	Internal forum- Review and update risks, Milestones and Delivery Plan	Oliver Sutherland (PMO) Sara Fouad (PM)
Weekly P2Pe Meeting	Wed 13:00	Weekly	External forum- Walk through prepared PPT to provide an update on progress to and from Fujitsu, Ingenico and Vocalink. Open forum for discussion to raise risks, issues and dependencies and new actions. Meeting is tracked via PPT.	James Foulk (PMO) Alex Wood (Solution Architect) Wayne Fitzgerald (PED Deployment PM) Oliver Sutherland (PMO) Sara Fouad (PM) Seb Schultz (FJ PM) Torstein Ogodeseth (Snr Architect) Paul Braisher (Architect) Leon Toland (IUK PM) Steve Broughton (Vocalink PM) Phey Rasulian (Programme Manager) [Optional]
P2PE Regular Tech Workshop	Wed 15:30	Weekly	External forum-Walk through prepared PPT to provide an update on progress to and from Fujitsu on low level technical discussions/designs. Open forum for discussion to raise risks, issues and dependencies and new actions. Meeting is tracked via PPT.	Alex Wood (Solution Architect) Sara Fouad (PM) Torstein Ogodeseth (Snr Architect) Paul Braisher (Architect) Seb Schultz (FJ PM)
PCI Architecture Overview	Thurs 10:00	Weekly	Internal forum- To provide the IT Security team with updates and progress made to date, as well as show casing PCI solution designs.	Dave King (Security Architect) Adam Malach (Head of Security) Syed Naqvi (PCI SME) Oliver Sutherland (PMO) Sara Fouad (PM) Alex Wood (Solution Architect)

Confidential

POL00423569

Communication plan – External

Meetings

External Parties: Global Payments, Qualified Security Assessor, Banking framework members

- *Monthly Updates*– Duration: 1-hour Location: Teleconference/ virtual

Post Office Attendees: Workstream leads, Programme Manager, Client relationship manager

Share and discuss progress against plan

Answer any questions that may be asked

External Parties: American Express

- ***Quarterly Updates- Duration: 1 hour Location: Teleconference/ virtual***

Post Office Attendees: Workstream leads, Programme Manager, Client relationship manager

Share progress against plan and any impact to critical milestones

Reports

- Regular client update presentation compiled and approved by the PCI communications working group

Confidential

Post Office Limited - Risk and Compliance Committee-06/05/20

POL00423569

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Cyber Security Strategy Update	**Meeting Date:**	06 May 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 our pursuit of agreed target maturity levels
- To note the status and plans regarding our response to the Cyber-related threats associated with COVID-19.
- To note the guidance for all RCC and ARC members regarding the secure use of social media.

Previous Governance Oversight

- Actions to report on 3 above topics occurred at the previous Risk and Compliance Committee (RCC) in March 2020.

Executive Summary

Good progress on achieving our target security maturity has been made. We are about to conduct a retest with Deloitte that will confirm this and help set the agenda for next year.

We have worked together with the wider IT, Communications and Data Privacy teams in balancing risk and availability of IT services to help ensure the Post Office can continue to operate during the COVID lockdown. We have also formulated specific responses to NCSC-identified threats around COVID-19

RCC & ARC member are urged to review their privacy settings and digital footprints using the guidance in this paper to ensure that they stay safe online.

CONFIDENTIAL

POL00423569

Questions addressed

1. What is our current Cyber Security maturity vs. target and what are our plans for 2020/21?
2. What are risks, issues and threats associated with COVID-19 and how have we dealt with them?
3. What do we all need to do to ensure our social media presence is secure?

Report – Cyber Security Maturity and Plans

4. Since we conducted the Deloitte Maturity assessment in March 2019 much progress has been made – Appendix 1 shows the current status. Our aim is to close as many of the actions by end April to ensure that we get as close as possible to target maturity values.

5. Our overall average maturity score across the 33 security capabilities assessed by Deloitte in March 2019 was 2.15 out of a maximum score of 5. Our agreed average target maturity at that time was 2.59. We estimate (we do not have access to the Deloitte toolkits to be definitive) that we will achieve an average maturity score of 2.4 by mid-April – we will have the final updates in shortly and will cross check them with internal audit. The shortfall in the maturity achievement is due to COVID-19 related and other delays in projects we are dependent on to support our increased capabilities.

6. We are starting a Deloitte-led maturity retest on 11 May 2020 to assess our progress. Rather than test areas where we have had a small gap to close or have made little progress, we have asked Deloitte to perform a more focused test aimed at 20 of the 34 cyber capabilities where there has been major progress in the maturity model. Deloitte will then update our scores based on those from the previous assessment and the scores from this assessment. We have also asked Deloitte to lead us through a reset of our target maturity at this time in line with changes in the Cyber threat environment and our new business priorities and operating model.

7. The resulting gaps will form part of the input to our 2020/1 cyber change programme which is currently in the process of being agreed. We will present details for this programme and the rationale for it at the next meeting.

CONFIDENTIAL

POL00423569

Report – Covid-19 Threats and our Response

Cyber activity relating to the move to our new operating model

8. We have updated COVID-19 specific cyber risks in partnership with the risk team and have pursued mitigation actions, described in more detail below.

9. Many in Post Office already have laptops and are used to using them both in and out of the office. However, those who only have desktops or have a laptop and have never really used it outside of the office have faced some user-related difficulties in accessing the Post Office through the Virtual Private Network (VPN) (which provides similar protection to working within the office when working away from it).

10. Some have had expired passwords which have needed to be reset away from the office To enable the move to remote working we have worked closely with IT operations to rapidly enable home working on laptops for people who have. This has required a pragmatic approach to security where some controls around password ageing have had to be relaxed temporarily to enable the Post Office to continue working.

11. There is a risk that with so many now working from home that, if users do not use the VPN to connect, they will not receive regular patches and updates to anti-virus placing their devices and others in the post office at risk. We have worked with IT operations on education and how-to intranet articles to reduce this risk by educating users on how to use the VPN.

12. Several Post Office users working from home for the first-time requested access to the ability to print at home. A solution for applying for home printing was developed jointly by IT, Data Protection and Cyber Security with instructions being place on the Digital Workplace intranet site.

13. Through our data loss prevention technology, we can monitor users who are sending documents to their home email accounts even away from the office. In addition to seeing the user details we can also see the specific documents that have been shared. In cases where the data involved is clearly commercially or personally sensitive then Data Protection and Cyber are following up with calls to the individuals involved.

14. The overall situation is being kept under careful observation with communications being sent out on the Post Office intranet site to advise users against sending any post office data to home email addresses.

15. We have also performed a short insider-threat type test of our service desk to ensure that, when performing a password reset then reset passwords are communicated securely. This has resulted in some minor changes in how the desk operates.

POL00423569

COVID-19 Threats and our Responses

16. The UK National Cyber Security Centre (NCSC) have characterised the cyber threats associated with COVID-19 as follows:

    a. **Phishing**, using the subject of coronavirus or COVID-19 as a lure
    b. **Malware distribution** using coronavirus or COVID-19 themed lures
    c. **Registration of new website domain names** containing coronavirus or COVID-19 related wording
    d. **Attacks against newly (and often rapidly) deployed remote access** or remote working infrastructure.

17. The aim of any **phishing** attack is to infect a machine with malware (possibly ransomware) by a user clicking on a link that causes **malware** to be downloaded to that machine. The results can be catastrophic e.g., Maersk shipping's 2018 near total loss of the company was caused by such an attack.

18. In late March we ran a campaign on phishing starting with comms/awareness going out on the Post Office intranet about how to spot it and what to do if you receive a phishing email. This was followed a week later by a fake-phishing attack using the offer of Covid-19 test kits (from a source purporting to be the NHS) as a lure.

19. The results of the attack were summarised in an all-staff email (see Appendix 2). We will continue to run such campaigns regularly in the future to boost staff awareness.

20. Through the use of our anti-phishing toolkit we have reported any suspicious emails to NCSC who have started a UK-wide campaign to collect and coordinate the response to such emails – more details here.

21. The registration of new website domain names containing COVID-19 has exploded I number with NCSC estimating that around 6000 new ones are being created a week. NCSC state "This is a fast-moving situation and this advisory does not seek to catalogue all COVID-19 related malicious cyber activity. You should remain alert to increased activity relating to COVID-19 and take proactive steps to protect yourself and your organisation."

22. In response our Security Operations Centre (SOC) has embarked on a proactive threat hunting campaign to find such "dodgy" websites and to blacklist them so that staff are unable to access them. We have found over 2000 such websites which have a post/postal element to them and have blacklisted them.

23. The SOC has also loaded the tell-tale signs (termed indicators of compromise) into our event monitoring platform (Splunk) so that we can see if there are any signs of the kinds of attacks associated with COVID-19 aimed at Post Office.

24. We have not introduced any new **remote access/ remote working** infrastructure of note but have instead leaned heavily on existing technology and measures.

POL00423569

25. We continue to focus on joiners, movers and leavers (JML) as detailed in the previous paper but progress on improvements has been interrupted somewhat by the immediate need to support a move to remote working. We are now reviewing our plans in the light of the likely hybrid operating model for Post Office to ensure that they have the correct focus and will report back in the next paper.

26. Finally, there is only so much that our technical controls can achieve. More than ever we need our people to participate in a more security-savvy culture now we are working in a remote fashion. Never has the new marketing-led strapline of "we're stronger together" seemed more apt for Cyber at Post Office as we all have a part to play. With that in mind we have embarked upon a more proactive communications and awareness programme with the assistance of the Central Communications team – more details to follow in July's paper.

Report – Protecting Ourselves on Social Media

27. Social media use is a routine part of daily life for many of us. In addition to the normal benefits it has become an essential part of life under COVID-19 restrictions. Like all technology it can be used for good and bad means.

28. In the previous paper details of the results from the recent red-team exercise revealed that it was relatively easy to harvest details of GE and Board members at Post Office from social media and other publicly available information. One possible use of such activity is to profile people so that criminals can then make an approach to coerce or bribe an individual either on-line or in person.

29. This kind of social attack can happen to anyone but the fact that GE and Board members are much more visible and have more power and influence than the average employee tends to make them more desirable targets.

30. Fortunately, there a range of actions that we can all take to protect ourselves which are

    a. Ensure that we consciously set the privacy settings on social media that we use. NCSC have published links to the specific privacy settings of the main platforms here.
    b. Ensure that we understand our digital footprint and where possible try to minimise it. Help on assessing and managing this is available from the Centre for the Protection of National Infrastructure (CPNI) here.

31. The information on each of these resources is clear and simple to follow but please feel free to contact Tony Jowett with any further queries you may have. Also, if you are approached with any untoward offers/suggestions then please get in touch so we can assist you.

POL00423569

Appendix 1 Security Transformation Programme Status

Area	Milestone Completion			Target Completion Date	Update
	Target	Previous	Current		
Deloitte Cyber Review Actions	90%	73%	83%	March 2020	Good progress of late, 31% of actions have been placed on indefinite HOLD as current strategy & COVID-19 changes have affected outcome
Deloitte Information Protection Review actions	90%	65%	68%	March 2020	Good Progress, it is still expected that all actions will be closed
RSA Archer implementation	40%	100%	100%	Feb 2020	"Cyber Security Assurance" and "3rd Party Cyber Assurance" are fully operational Central Risk team are now system owners
DLP Overall System	80%	70%	70%	Feb 2020	DLP Policy – 100% MCAS – 100% AIP – 30% (Test stopped) InTune – 100%
DLP Policy DLP MCAS DLP AIP DLP Intune	DLP policy engine is fully operational since Oct-19, only in Monitor mode, no enforcement other than SOC and DPO processing alerts generated by DLP. An enterprise wide analysis will be required in 2020 to review business operations that fall foul of DLP that require addressing for enforcement mode to be enabled. MCAS (MS Cloud App Security) System has also been fully operational since Nov-19 AIP (Azure Information Protection) document classification, testing failed due to a comparability issue with POL old deployed Office versions, this is now on hold until the EUC refresh addresses the Office updates. InTune is currently in operation and security enhancements and updates are integrated as part of BAU change and EUC				
SOC Maturity	Treated as ongoing continual improvement to BAU. Widening coverage of SOC through acquisition of more logs including Payzone and Post Office Insurance. Red Team events planned for 2020 to further develop SOC				

CONFIDENTIAL

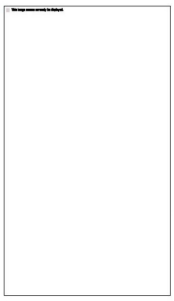
POL00423569

Appendix 2 – Communications from Results of Fake Phishing Attack

one update

8 April 2020 | Reading time 2 minutes | For information and action

5



Hi everyone,

It's important for everyone to really recognise that we are more reliant on our IT staying safe and secure than ever, as we adjust to our new ways of working at this unprecedented time. Of course, this also means that the risks are higher and the consequences greater (e.g. there are no easy or quick ways to investigate or replace laptops). Please always be mindful of attempted or potential phishing attacks especially when we are all working under increased pressure with increased distractions.

Phishing exercise

To test our readiness, last week, the Cyber Sec team ran a Phishing exercise (relating to COVID-19) which simulated real attacks that are happening now. Here are the headline results:

Emails sent	**4,184**
Total colleagues reporting as a scam	1,184 (28%)
Total colleagues "lured"	*439 (11%)
Post Office security measures initiated	75 seconds
Total colleagues lured before mitigation	**21** (0.5%)

**this included one GE member – no-one is immune.*

The two critical measures to note are time taken for our security measures to recognise this specific attack as dangerous (75 seconds) and the number of colleagues who clicked or opened the attachment BEFORE these measures kicked in: 21. At best, this means we would be dealing with 21 infected machines. If the payload from the attack included ransomware, then any one of those infections could easily result in a serious hit on our ability to operate as an organisation.

I appreciate that we're all working under increased and unforeseen pressure – but attackers know this too. And indeed they are relying on it... so the best advice we can give is to stop and think before you click. If

CONFIDENTIAL

POL00423569

you have any doubt, then report "dodgy" emails by clicking on the IronScales button on Outlook (if this fails, please forward the email onto ISSAPOIT GRO .

Always question emails where you do not know the sender or were not expecting something. You can always contact us at information.security GRO for assistance.

Within Cyber, we are going to continue to undertake these and similar test attacks over the coming weeks and months – and we'll continue to report back the findings.

I'll be starting a more regular pattern of communication over the coming weeks, to bring to life and highlight some of the tactics used by attackers, some of the more sophisticated patterns of attack and to provide you with advice for use both at home and at work.

Think before you click.

Tony Jowett

CONFIDENTIAL

POL00423569

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Progress Update on the Pilot Implementation of the Contract Management Framework	**Meeting Date:**	06 May 2020
Author:	Sherrill Taggart, Group Legal Director	**Sponsor:**	Ben Foat, General Counsel

6

Input Sought:

The Risk and Compliance Committee ("RCC") is asked to **note**:

- The implementation of the pilot of the Contract Management Framework ("CMF") will, as planned, complete on 19 May 2020.
- The projected final costs of the pilot.
- The costs, timeframes and residual risk associated with the post pilot options for the implementation of CMF across the Post Office Group ("PO Group") presented within this paper.

The RCC is asked to **approve for recommendation to the Audit, Risk and Compliance Committee** ("ARC"), the recommended approach:

- While internal training has been provided, accredited external training will not be provided to identified contract managers for material contracts, accepting the risk that this may result in a baseline level of capability not being established amongst this group of individuals.
- Reallocating £26k of the £80k originally included in the budget to provide external training in order to complete the upload and mapping of all remaining contracts identified by GE as being material in terms of strategic and financial value by the end of June 2020 ("Material Contracts").
- It is proposed that the implementation of CMF across those contracts not identified as being material by the Group Executive ("GE") ("Other Contracts") be done outside of this project through the natural 'lifecycle of a contract' e.g. as they are renewed, cease or new agreements are entered into. This will take significantly longer, through BAU resource and processes, but release c£700k from the 20/21 Change Portfolio Budget.

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

Confidential

POL00423569

Executive Summary

The implementation of the CMF pilot will complete on 19 May 2020[1]. At the ARC meeting in March, the project team offered to return to the ARC in May 2020 with options regarding the wider rollout of the implementation, following the completion of the pilot.

Against the original target of identifying, uploading and mapping obligations for 50 Material Contracts with funding of £300k - by the end of the pilot we expect to have spent £100k, uploaded and mapped the obligations for 60 Material Contracts and to have identified benefits of c£440,000[2].

This however leaves circa 82 Material Contracts and circa 1,500 Other Contracts which will not have been uploaded onto Web3.0, nor had their obligations mapped or benefits identified.

To complete the implementation for all Material Contracts (142 in total) would take one additional month and cost £26k. It is estimated that it would take at least a further 6 months and £330k to complete the implementation for all the other circa 1,500 contracts.

Given the current commercial environment within which the Post Office is operating, the recommended approach is to complete the implementation for all 142 Material Contracts, but not extend the implementation into the remaining contracts. It is understood that the Source 2 Settle Programme is seeking funding to upload the static data associated with the 1,500 Other Contracts (i.e. start date, end date etc.) but not to map the obligations, set automated alerts etc.

Questions addressed

1. What progress has been made with the pilot implementation of the CMF since the last update provided to the ARC in March 2020?
2. Once the pilot is completed, what options exist in relation to a wider implementation and what are the associated timeframes and cost?
3. What is the recommended approach?

Report

1. At the November 2019 meeting, the ARC approved a cost efficient, decentralised framework for contract management across the PO Group. It also approved (i) the implementation of the CMF being piloted with the top 50 Material Contracts and, (ii) subsequent to a dependency on a confirmed GE and GE-1 structure, the duration of the pilot being extended to 19 May 2020, in part owing to there being no impact on the budget.

2. Progress against the deliverables set out in the Prove Plan are set out below:

Measurement	Original Target	Current Position	Forecast Position at Closure (19 May 2020)
No. of Material Contracts identified	50	142	142

[1] The scope of which (as set out in the associated Prove Plan) is included at Annex 3.
[2] Through rebates due to Post Office as a result of Legal Spend

Confidential

POL00423569

Measurement	Original Target	Current Position	Forecast Position at Closure (19 May 2020)
No. of Confirmed Latest Versions of Material Contracts	All (142)	91	142
No. of Material Contracts with Contract Managers	All (142)	118[3] (managed by 43 Contract Managers)	118
No. of Contract Managers On-boarded & Trained via the LCG Academy	All (43)	38	43
No. of Contract Managers Trained by the IACCM	All (43)	0	0 (though all will have received internal training via LCG Academy)
No. of Contract Managers 20/21 Objectives to include Contract Management	All (43)	39	43
No. of Material Contracts Uploaded onto Web 3.0	50	44	65
No. of Material Contracts with Obligations Mapped	50	44	60
Rebates identified & Realised	Not Quantified	£436,000	£436,000
Other Value adds Identified	Not Quantified	• 7 contracts with Service Credit Provisions. • Ability to move quickly during CV-19.	
Spend vs £300k approved	£300,000	£38,000	£100,000 - £180,000[4]

6

4. In addition to the numbers set out above, 13 Other Contracts have also been uploaded onto Web 3.0 and had their obligations mapped. The full list of Material Contracts which have been mapped, and those Material Contracts for which we have not yet located a confirmed latest version of that contract (with all ancillary documents) is included at **annex 1 and 2** respectively.

5. The RCC will note that although the project will exceed its target to map the obligations for 50 Material Contracts by 19 May 2020 (the completion date for the pilot), there will still be a significant number of Material Contracts which the PO Group is party to which will not have been uploaded onto Web 3.0 platform, nor had their obligations mapped.

[3] Of the 24 material contracts without contract managers, this is in large because of the ongoing structural changes
[4] The reason for the delta (c£81,000) is the difference between providing external training or not. Other material savings which have been made against the original budget include £30k in external legal advice, £15k in programme resource costs, £20k in licence fees and the quote from the external training providers was £30k below the original provision.

POL00423569

6. The following options are available to the ARC:

External Training for Contract Managers of Material Contracts

Within the approved budget for the pilot was a provision for accredited external training. The external training would create a common contract-management language, knowledge-base and baseline level of capability across the PO Group. The associated accreditation is based upon the Contract Management Professional standards as endorsed by the Government Commercial Function, International Association for Contract & Commercial Management, and the Chartered Institute of Procurement and Supply.

Post Office is not however committed to this spend and we have paused the associated CAF process, pending a decision by the RCC and ARC. Not proceeding with this spend would release approximately **£80k** of the budget which could be released back to the business or re-purposed to deliver the options described below.

Option	Timeframe to Complete	Cost Implications	Residual Risk	Recommended?
1. End pilot on 19 May 2020 with **no** further implementation of wider rollout	Pilot ends on 19 May 2020	Ending the pilot on 19 May 2020 with no further wider implementation will result in savings of either: • £120k against the original 300k of funding provided, if the decision is taken to still provide external training to contract managers of material contract; or • £200k if the decision is taken not to provide the external training.	• c82 material contracts won't have been located, uploaded onto Web 3.0, nor had their obligations mapped and benefits (service credits, price reviews, rebates etc) identified. • The same will be true of c1,500 Other Contracts which we believe Post Office to be party to. For these contracts, Post Office will be exposed to the risks described in previous papers to the RCC.	NO
2. Complete the implementation for all 142	• We expect to be able to locate,	• The current run rate for the programme	• Post Office would not have the	YES

Confidential

POL00423569

Option	Timeframe to Complete	Cost Implications	Residual Risk	Recommended?
material contracts with no further implementation or rollout thereafter	upload onto Web 3.0, and map the obligations for all 142 material contracts by 30 June 2020[5]. • For speed, the obligation mapping may however have to be done without the contract manager.	(excluding external training costs) is c£26k per month. • Thus, this exercise would cost c£26k to complete, which could be offset by the projected £120k – £200k underspend described above.	complete picture of its contractual landscape, and be exposed to the risks described in previous papers to the RCC, albeit for only those contracts deemed not to be material. • Over time, this would remedy itself as non-material contracts are renewed / expire / new agreements are entered into.	
3. Complete implementation for all 142 material contracts and all c1,500 non material contracts	• This would be a significant undertaking and require a programme to be appropriately resourced and funded for, at a minimum, 6 months	• Current resource levels would need to increase from 1 PM and 2 paralegals to 1 PM and 6 paralegals[6] • This would result in monthly run costs increasing to c55k per month – an additional cost over 6 months of £330k	• All current contracts which Post Office is party to (material and non material) would be uploaded onto Web 3.0 with their obligations mapped. There should not, therefore be any residual risk through adopting this approach.	NO

7. Given the current challenges faced by the Business, the recommended approach is:

[5] With 4 contracts being uploaded and mapped each day (2 per paralegal). Thus, c20 per week and c80 per month.
[6] With 12 contracts being uploaded and mapped each day (2 per paralegal). Thus, c60 per week and c240 per month.

POL00423569

- Not to proceed accredited external training to those individuals identified as contract managers for Material Contracts, accepting the risk that this may result in a baseline level of capability not being established amongst this group of individuals.

- Re-allocate £26k of the £80k originally included in the pilot's budget to complete the uploading and mapping of all Material Contracts, accepting the risk that the PO Group will not have a complete picture of its contractual landscape in respect of the circa 1,500 Other Contracts. It is understood that that the Source 2 Settle Programme is seeking to raise a change request to fund the uploading of the circa 1,500 Other Contracts– albeit from a static data perspective only (i.e. start date, end date etc.) as opposed to mapping obligations, setting automated alerts etc.

- That the implementation of CMF across those contracts not identified as being material by the GE be done outside of this project, as part of BAU as contracts are renewed, cease or new agreements are entered into. This will release c£700k from the 20/21 Change Portfolio Budget.

Confidential

POL00423569

Annex 1 – Material Contracts Mapped

	Contract Name	Other Party
1	An on-line advisory service	Adviser plus
2	Affilliate Management	AWIN
3	Agreement for the Provision of Money Transmission Services	MoneyGram Payment Systems, Inc
4	AllPay Bill Payment Agreement	AllPay
5	ATM agreement	Bank of Ireland
6	Audit of Notes Circulation Scheme, MDA, DVLA BIS loan	PWC
7	Back Office IT Tower contract	Accenture
8	Banking Framework (& Banking Framework 1.3)	Various
9	BT Bill Payment Agreement	BT Telecommunications plc
10	Car, Van and Home Insurance	Budget Insurance Services Ltd
11	Common Digital Platform Agreement	Accenture
12	Creative Agency	Ogilvy & Mather Group (Holdings) Ltd
13	Crown Transformation - Self Service Kiosks (SSK's)	NCR Ltd
14	DAM tool	Splash
15	Duck Creek Policy	Duck Creek
16	EDF Bill Payment Agreement	EDF Energy Customers plc
17	End User computing (provision of equipment & support/maintenance)	Computacenter
18	Financial Services Joint Venture Agreement	Bank of Ireland
19	Front Office Counter Services (FOCS) Framework - Framework Agreement, DVLA Call Off, DVLA Extension and Novation to Crown Commercial Services	Crown Commercial Services
20	Retail Arrangement Agreement	WHSmith (supply of stationary and packaging in our branches
21	Grant Agreement- Support NT	NFSP
22	Home Insurance	Ageas Insurance Ltd
23	Horizon IT hardware, application, data centre and network services	Fujitsu Services Limited
24	Interims and Contractors	Intelligent Resource
25	Life Insurance	Royal London Life Contract
26	Media audit	Ebiquity
27	AEI Contract	Thales
28	O365 Services &Products	Microsoft
29	Portfolio & Service Management (Including IT Helpdesk)	Service Now
30	Ped (Pin Entry Device)	Ingenico UK Limited
31	Network IT Tower contract	Verizon
32	Paystation Agreement	Ingenico
33	Pension provider - Money4Life Service Agreement	Zurich
34	POL's Outsourced Contact Centre (Home Insurance) (POMS)	Firstsource Solutions UK Ltd
35	POL's Outsourced Contact Centre (Travel, General Insurance and other Products) (POMS)	Telecom Services Centres Limited t/a Webhelp
36	PowerNI Bill Payment Agreement	PowerNI
37	Private Medical Care Insurance Provision	Bupa
38	PwC external audit	PWC
39	Grant Thornton 3rd party data audit	Grant Thornton
40	Technology Services	Accenture

Confidential

POL00423569

41	Travel Insurance	Ergo Travel Insurance Services Limited
42	Travel Insurance	Collinson Insurance Services Ltd
43	Verify ID Checking	Digitentity
44	Verify ID Checking	DWP (Cabinet Office)

Annex 2 - Material contracts for which we are still locating a confirmed latest version of that contract

Kindred	Lord Mayor & Citizens of Westminster/ Hammersmith & Fulham Borough Council	FRES : FSJVA
BT Telecommunications : Services relating to Bill Payment	Servest	FRES : International Money Transfer
Capita: Travel & Events	Royal Mail : Swindon Warehousing Agreement	CBRE
Eon	POMS : MSA	BNP Paribas
ePay	Verizon: Core Telecoms Network	Kings Security Ltd
SAP UK Ltd : Master Agreement	KPMG Nunwood	Insafe International Ltd
nPower	Quadrangle	Santander
Ingenico	Trinity McQueen	Santander : Payout
Scottish Power	Kantar	British Gas: Bill Payment
SSE Energy	ABA	GPUK
Yorkshire Water	GFK	Mediazest
Capita Travel	Kouros	
Postmaster/Main/Local : Agency and Branch network	Vocalink Ltd	1) Key Fuels (CH Jones) – Fuel Card Provider 2) Harvest Fuel – Main Supplier Fuel for forecourts. 3) Enfilade – Tank Management 4) Allstar – Fuel Backup Card 5) Portland Fuel Fuel Trading Company – Provide Fuel Hedging
POMS : Distribution Agreement	CWU	
BEIS : Government funding provision of network	Unite	
BEIS : Entrustment	FRES: Foregin Currency Exchange	
Royal Bank of Scotland	WorldPay	1) Belfast Bunker = LCC Fuel 2) Birmingham = Certas Energy 3) Hemel = Watson Fuel 4) Newcastle = Certas Energy 5) Norwich = Watson Fuel
UKGI	ATOS	
McKinsey & Company Inc UK	Bank of England (Note Circulation)	

6

Confidential

POL00423569

Annex 3 –Pilot Scope

- Identify and ratify with GE & the Business the top 50 material contracts based on financial and strategic value and risk profile.
- Identify contract owners and contract managers for the top 50 material contracts.
- Map out roles and responsibilities for contract managers and owners.
- Identify and agree KPIs for contract managers and owners.
- Review the job descriptions and objectives of identified contract owners and managers.
- If required, amend job descriptions and objectives of identified contract owners and managers where necessary.
- Identify the appropriate suite of training to be provided to the top 50 material contract owners and managers.
- Deliver training on core skills and Web 3 (Source to Settle (S2S) to contract owners and managers of the top 50 material contracts.
- Upload top 50 client/supplier contracts on to S2S.
- Map the obligations for top 50 client/supplies contracts.

Confidential

POL00423569

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Horizon Scanning Report	**Meeting Date:**	6 May 2020
Author:	Sherrill Taggart (Legal Director)	**Sponsor:**	Ben Foat (Group General Counsel)

Input Sought: Noting

The Risk & Compliance Committee (RCC) is asked to note the new or proposed material changes to laws and regulations this month.

7

Executive Summary

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

1. Streamlined Energy and Carbon Reporting Update;
2. Morrisons Supreme Court Appeal;
3. IR35 'Off-Payroll' Rules Update (Covid-19);
4. Employment Legislation Update (Covid-19); and
5. Business Area Update (Covid-19).

Those matters that relate to Covid-19 are continuously monitored to assess the short and long term risks and potential impact to the Post Office through the relevant working groups that have been stood up and a robust governance framework.

With regard to the other matters referred to, significant work has already been undertaken to ensure any material risks that may arise for the Post Office are being managed to ensure compliance. Where no action is required, the matter has been noted and any further developments will be reported on.

POL00423569

Appendix 1

1. RCC Horizon Scanning Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action
Streamlined energy and Carbon Reporting Update ('SECR')	In April 2019, the SECR scheme was introduced under the Companies Act 2006 and imposed greater reporting obligations than the previously abolished CRC Energy Efficient Scheme. Under SECR, Companies now are obliged to report on vehicle emissions and also provide a narrative commentary on any energy efficiency action taken in the previous financial year.	The scheme came into force April 19 and therefore April 2020 is the first reporting cycle under SECR.	Post Office are expected to report under the SECR the following items: - Electricity usage; - Gas usage; and - Transport emissions. Post Office hasn't previously reported on transport emissions and therefore operational changes were required in order to collate this information to report on. Post Office's property team instructed Inspire to collate the data required for Financial Year 2019/2020 and prepare the SECR report that will be used in the Annual Report and Accounts. The narrative of initiatives implemented also sets the baseline for future annual reports and sets out the objectives by which Post Office will measure against over the next ear. PWC have assured Post Office that as a company we are ahead of other client's and there has been relative comfort over the figures shared.	A draft report has been shared with Al Cameron and a final report was sent to PWC for review on 22 April. We are expecting their feedback during week commencing 4 May.
Morrisons Supreme Court Appeal	In a Court of Appeal decision, it was found that organisations could be vicariously liable for data breaches caused by rogue employees, even where an organisation had taken appropriate measures to comply with data protection obligations. This decision would have set a precedent for future victims of data breach breaches to argue an employer is vicariously liable for the actions of a former employee and	Morrisons appealed the decision made by the Court of Appeal, and the Supreme Court found that the decisions of previous courts and the Court of Appeal were 'contrary to the established approached to questions of this kind, and were based on a misunderstanding of this Court's decision'. The Supreme Court found that the test of vicarious liability is limited to circumstances where actions of the employee were carried out in the pursuing the business of the employer and were not in an effort to	Although vicarious liability is not new law, this Supreme Court finding provides helpful clarification on the potential scope of vicarious liability as it may apply to 'rogue employees' and 'insider threat scenarios' in the context of data breach incidents. In light of the first Court of Appeal decision back in 2018, Post Office reviewed its approach to Joiners, Movers and Leavers and highlighted several weaknesses. A project was undertaken to address these weaknesses and several changes were made	There is no action required by Post Office following the Supreme Court Decision. The decision does provide comfort in regards to 'rogue employee' in the context of data breaches, and Post Office will continue monitor for any further guidance published as a result of this decision.

Strictly Confidential

Post Office Limited - Risk and Compliance Committee-06/05/20

POL00423569

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action
	exposed organisations to group claims where this had occurred.	deliberately harm the employer, as in the Morrisons Case.	to a variety of IT policies to implement these. This was previously reported on at RRC in detail by Jonathan Acres.	
IR35 'Off-Payroll' Rules Update	IR35 is tax legislation aimed at combatting tax avoidance by workers who supply their services to clients through an intermediary but who would be taxed as employees if engaged directly. Although this legislation was in place for over 17 years, compliance was low and the Government set to change the way in which the legislation operated. The new legislation was due to come into force on 6 April 2020, however many private organisations have raised various concerns with the new legislation. The Government announced a review into the IR35 rules which provides an opportunity for stakeholders to demonstrate quite how damaging the rules might be.	Due to various factors arising from COVID-19, the Government made the decision to delay the implementation of IR35 until April 2021.	Post Office has had to comply with the IR35 rules since April 2017 given the applicability to public sector organisations came into force previously. Therefore there has not been a big impact compared to other businesses, however it has provided Post Office a chance to ensure we were complying with the rules correctly and provide the opportunity to correct historical mistakes, for example going forward earlier contact will be made with line managers regarding their contractors who are approaching the two years of engagement with Post Office in order to ensure effective resourcing and sufficient time for replacements to be found if necessary. 22 individuals were flagged as an IR35 risk, all have been dealt with having either moved to full time positions, exiting the business or being placed an inside IR35 contract. The decision to delay the implementation of IR35 has therefore had minimal impact to Post Office, with the only practical change being that Post Office are no longer required to inform upcoming contractors whether they are inside or outside of IR35. However, as best practice Post Office has made the decision to do this anyway.	The minimal impact of the delay has meant there is no immediate action for Post Office however work has now completed on an historical audit of all the previous decisions regarding IR35, and it found all decisions were found to be compliant. As the position currently stands, 9/66 contractors are on contracts inside of IR35.
Employment Legislation Update (COVID-19)	Due to the impact of COVID-19, there have been many legislative changes in the employment landscape in order to accommodate and effectively react to the changing requirements. The Coronavirus Act 2020 was introduced by the Government on the 19 March and came into force on the 25 March. The Act introduces emergency powers to handle the COVID-19 pandemic, and out of this introduces several employment changes.	Of those that will be most applicable to Post Office: a) Coronavirus Job Retention Scheme ('JR Scheme') – The JR Scheme was introduced to support businesses and employees affected by COVID-19 where employers were unable to maintain their current workforce. Employers could apply to the Government for a grant covering up to 80% of its usual monthly wage costs. The JR Scheme launched on 20 April, and as it stands currently will run until 30 June;	a) Whilst the Government has announced it does not expect many public sector employers to use the JR Scheme, it does acknowledge that, in some cases, it may be appropriate and with BEIS approval, POL may be able to use the JR Scheme. At the current time, no decision has been made to furlough Post Office staff but the option is being considered alongside other options to redeploy employees where they are not being fully utilised.	a) No further action necessary, the JR Scheme is being considered alongside other options. Continue to update the employee FAQs as and when necessary and assess impact.

POL00423569

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action
	There has also been changes made to existing employment legislation.	b) Emergency Volunteering Scheme ('EV Scheme') – The Coronavirus Act included provisions for the introduction of a new temporary statutory right to emergency volunteering leave. The provisions will need secondary legislation to be passed before the EV Scheme becomes law, however the expectation is that this will occur imminently. Once the law is passed, a worker with a valid emergency volunteering certificate (for example an NHS Body or Department of Health) will be able to apply for unpaid emergency volunteering leave. The EV Scheme will apply for an initial 16 week period, allowing workers to take one period of volunteering leave of two, three or four complete weeks with a minimum of 3 working days' notice;	b) Post Office are currently keeping a watching brief on the passing of any secondary legislation. However as it stands, there is no right to refuse a request and therefore Post Office will have to accommodate any that might come through. There are certain exemptions for small employers, civil service and the police however Post Office currently is not listed as an exempt employer and therefore expects to be subject to the legislation. There is however a provision for the Secretary of State to add to the list of exempt employers which may change this. It is important to note that this is not a blanket right for all volunteering activities during the coronavirus to take unpaid leave, rather those who are required for a specific period because they have suitable medical or social care skills.	b) Watching brief over any secondary legislation that formally introduces the EV Scheme as law. Post Office will continue to assess the impact the EV Scheme might have and continue to update the employee FAQs as and when necessary.
		c) Working Time (Coronavirus) (Amendment) Regulations 2020 – Carry-over of Annual Leave – Under EU Law all workers are entitled to 28 days annual leave (including bank holidays) each holiday year, although Post Office enhances this entitlement, 20 days of each employee's annual entitlement is statutory holiday. Usually, this holiday has to be used in the relevant holiday year and days can only be rolled over if someone has been too sick to take their holiday entitlement. The Government has recognised that due to the response to COVID-19 some employees may not be able to take their holiday entitlement. Due to this fact, where it is not reasonable practicable for someone to take some or all of their leave due to the effects of coronavirus, carry over of the 20 statutory days' holiday will be allowed for up to 2 years; and	c) Post Office will be required to carry over the 20 days' of statutory leave however a decision has not yet be made about carrying over of holiday over and above 20 days. It is not anticipated at all staff will be affected by this, as only those who are unable to take leave due to their required ongoing contribution would be able to roll over their unused holiday entitlement.	c) Post Office will have to make a decision on whether carry over of above and beyond 20 days will be permitted. Full impact still remains to be assessed and what processes may need to be put in place in order to facilitate carrying over of higher amount of days. Further guidance to be published for employees as and when necessary.
		d) Gender Pay Gap Reporting Postponed – At the end of March, The Government Equalities Office and the Human Rights Commission announced that enforcement of	d) Post Office usually publish their figures at the end of March, however we haven't published this year's figures as of yet. It is unknown at this time whether Post Office	d) No action required.

POL00423569

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action
		the gender pay gap reporting requirements would be suspended for this year due to the unprecedented uncertainty and pressures which employers are feeling due to COVID-19. The decision came only 10 days before the deadline to report and at that time only 26% of employers had published their reports. Many more employers may have also already run their numbers and may still publish their results anyway albeit perhaps after the usual April date.	intent to publish anyway, or whether this year will be skipped. It is worth mentioning that the expectation is that next year's reports could be radically different given reports are based on snapshot data taken on 5 April each year. Many employers may have already furloughed staff, reduced their pay or hours which will impact their data. Although Post Office hasn't undertaken any of these activities and therefore data won't be affected, it is important to note when comparing against other companies next year.	
General updates across business in light of COVID-19	The impact of COVID-19 has been felt in all areas across the business and it important for the business to remain responsive to these changes and keep updated as the landscape continues to evolve and change.	**Compliance** It has become clear from the regulators that all rules and regulations still stand as they were and a focus has been on tackling new scams that have arisen taking advantage of vulnerable customers. Several consultations were expected over the coming months, and these have been postponed due to other priorities.	**Compliance** Post Office continues to ensure that vulnerable customers are being protected and it is reacting efficiently to the changing landscape. Senior members of Post Office met with Ofcom and discussed the approach to ensure that Post Office was dealing with the changing environment and could react to increased calls from customers, as the offer of forbearance has been exercised by customers across the various financial services products. The issues facing vulnerable customers at this time has also led Post Office to announce several access to cash schemes in order to address this.	**Compliance** The situation is being closely monitored and regular meetings taking place to ensure that the impact to the business is being managed efficiently through sufficient resourcing, implementation of new schemes and support provided The team will continue to update at the relevant forums and provide updates
		Financial Crime In March, Post Office saw the highest level of SARS since last June, with issues still being identified relating to cash deposits, and investigations are currently underway in 28 branches. From a regulatory perspective there is a reasonable amount of forbearance and understanding in complying with regulations. Supervisory activity has been suspended, however the situation is being closely monitored.	**Financial Crime** Sally Smith is attending a bi-weekly meeting with various stakeholders in the industry, including UK Finance that is looking specifically at new scams and issues arising from COVID-19 that target vulnerable customers. There is some concern that once lockdown is over there will be a large amount of cash arising from illegal activity that hasn't been banked, and this will arise in more people looking to take advantage of products with a risk of financial crime. From a regulator perspective, Post Office did not send agent data to HMRC in April and is proposing that this will remain the case in May also.	**Financial Crime** The situation is being closely monitored and regular meetings taking place to ensure that the new issues arising from COVID-19 are appropriately dealt with and Post Office is in a position to tackle the concerns once any restrictions are lifted The team will continue to update at the relevant forums.

Strictly Confidential

POL00423569

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action
		Post Office Insurance The Financial Conduct Authority ('FCA') has introduced many measures and provided guidance in many areas of insurance. Most recently the FCA have decreed that where insurance cover has been taken out in one period and there was a reasonable expectation that this cover was to be renewed, customers have a right to the renewal on the same terms and conditions. The FCA has also delayed several consultations back to 1 October 2020 and has also delayed the implementation of signposting rules for medically impaired customers discussed at the last Law and Trends Forum, with no new date being given. Regulatory and public pressure is also being felt as motor insurance firm, Admiral, announced a refund of £25 for their 4.4 million customers due to a reduction in vehicle use due to lockdown.	**Post Office Insurance** Any clarifications from the FCA regarding products Post Office Insurance offer will require action and implementing. Post Office Insurance are ensuring that customers are aware of changes and ensuring where there has been changes in circumstance customers are still covered when appropriate.	**Post Office Insurance** The situation is being closely monitored and regular meetings taking place. The team are working to ensure that clarifications from the FCA regarding products are implemented and that there is support for the customers as changes are introduced. The team will continue to update at the relevant forums.

POL00423569

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Supplier Contracts out of Governance	**Meeting Date:**	6th May 2020
Author:	Barbara Brannon, Procurement Director	**Sponsor:**	Alisdair Cameron, Group Chief Financial Officer

Input Sought: Noting

Noting – For discussion and further action if required.

Previous Governance Oversight

- March 2020 - Quarterly Risk Report

Executive Summary

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.

8

The purpose of this report is to set out both breaches to Post Office governance and key controls around contracts and compliance to PCR regulation in the award of contracts.

The aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Since the last RCC report in March, Board has requested prior approval of all Exceptions >£189k in a revision to existing governance. A Procurement Risk Exception Note will be required to accompany all Exception Requests and a Legal Risk note for requests >£500k, with Exemptions or with Medium/High Risk of challenge.

STRICLTY CONFIDENTIAL

POL00423569

Questions addressed

1. *How many and what types of procurement non-compliance have occurred in the past quarter?*

Since the last RCC report at the beginning of March there have been 13 non-compliant incidents:

a) 4 are direct awards under Regulation 32 for Covid19 operational response. These are assessed as Low Risk under PCR Regulation 32 due to unforeseen circumstances etc.
b) 3 legacy software support contracts which make up the Swindon Galaxy solution. This is an end of life system scheduled for replacement. Alternative support options are not available within the market due to IPR, and the age of the systems involved which are no longer commercially available. These are the subject of an existing IT/Supply Chain REN and remediation planning on the system is underway within IT.
c) 2 tactical short-term extensions 30-90 days to allow contractual negotiations to conclude on compliant contracts.
d) 1 Professional Services agreement in respect of Horizon System Strategy
e) 1 direct award on specialist marketing software.
f) 2 Contract extensions required in order to complete procurement processes [Media Planning & Global Payments]

A list of these awards is set out at the beginning of Appendix A.

2. *What are we doing about it?*

Active reviews continue with Business Units with the highest values relating to non-compliance.

Our overall non-compliance value has reduced from £21.01 in March to £19.5m in May.

This was driven by the completion of in-flight procurement processes offset by Covid19 operational response direct awards [PPE and Cash support] and two high value interim contract extensions required while tender processes are underway. These have been assessed as Low Risk and/or fall under Regulation 32 exemptions.

A visual breakdown on Open incidents is available in Appendix A.

3. *What is in the current Procurement pipeline which is high value and at risk of being awarded or extended non-compliantly?*

a) £10m. **EUC** - A project has been initiated to re-procure End User Computer services for both Branch and Colleague Services. The current plan is to have a new supplier(s) in place before the end of the current contract [April 2021 with 2 years exit services] with a targeted migration by April 2021. The project is currently gathering requirements to go to market however funding is constrained and some key resources have been diverted due to Covid19 operational responses.

POL00423569

b) £5m. **Common Digital Platform** - This is a tactical 2 year DOS contract which was let in June 2018, with a compliant six month extension option to Dec 2020 on a short term basis to allow for cloud migration and long term strategy adoption. At 31 December 2020 there is a hard stop with no Exit assistance period. Discussions are underway with the supplier to trigger the compliant six month extension option while procurement process(es) are run. CDP hosts a number of services including the external commercial website and the longer term strategy is to include the replacement services in the cloud convergence project with a possible insourcing of some service elements. Therefore, the current final scope of the re-procurement is under discussion. A short- term extension may be required in order to exit the remaining scope of services in early 2021. Detailed transition planning is underway but it would not be optimum to migrate during peak trading period at Christmas.

c) £1.3m. **Brands/Rapp** – this expires in November 2020. A business strategy, funding and sourcing plan needs to be agreed.

d) £5m. **Identity Services** – a paper went to GE in March outlining POL options to re-procure services which will end in November 2020. This is now critical path if POL wishes to continue as a supplier to Verify. Due to Covid19, negotiations were reopened with the incumbent provider to extend to March 2021 but these have not as yet concluded. Preparations continue on the OJEU RFP as new commercial business will be secured on certainty of POL supply chain in this respect.

e) £350k. **ATM Support** - A number of interim ATM support contracts expiring in August 2020 may need to be extended non-compliantly while the ATM tender process continues.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk.

Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate and/or available.

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

Report

4. What are the potential consequences of non-compliant awards?

a) Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.

POL00423569

b) Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

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

Non-compliant awards may be made for a number of reasons at the Post Office.

a) Low value, time constrained or highly sensitive/specialist engagements are not uncommon.
b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy and/or completion of large, and complex technical programmes of work to maintain or enhance services prior to a possible exit.
c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
d) Delays to public sector panels of suppliers becoming available. The Post Office makes extensive use of this low-cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
f) Disregard for, or lack of understanding of the regulations.

6. Why are we receiving this report?

A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However, it should be noted that it will facilitate timely responses to Freedom of Information requests which adds risk to the Post Office commercial landscape.

7. Are any of these breaches arguable on regulatory grounds or are they all breaches?

A full explanation of the individual compliance breaches for direct awards over £189k [previously £164k & £181k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach. The threshold is altered annually based on the FX rate between GBP and the Euro.

The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary, under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Approval Form [CAF].

All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires

POL00423569

at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

8. How many of the breaches were approved in advance and how many retrospectively?

All contracts entered into during this period were compliant with internal governance processes on contract and commercial review.

9. Why were the approvals given?

The rationale for approval is relevant to the individual service and is detailed within Appendix B.

10. What were the unapproved, material breaches?

There were no unapproved, material breaches during this period.

11. Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with their key stakeholders. The maturity of this look ahead view does vary currently and is consistently a high priority activity within the team.
b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are actively involved helping to advise and review options as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member now receives a regular report on compliance within their business unit[s].
e) A Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with GE sign off.
f) Awards over £189k must have prior Board approval before being entered into.
g) All Professional Services engagements must be approved in writing in advance by the CFO/COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
h) Procurement provides training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and a new training module made available on Successfactors. Ad hoc training sessions for interested Business Units are also run.
i) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
j) A revised POL Procurement Policy and supporting processes is in progress giving more granular guidance.
k) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.

POL00423569

l) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues e.g.: contractual value thresholds.

Risk Assessment, Mitigations & Legal Implications

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £189k.

Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Contract and financial governance policy and processes at Post Office are set by the Legal, Risk and Governance team with clear guidelines for staff availably on the Company Secretariat team intranet site. This sets out steps to be taken to obtain financial and contractual approvals prior to making a binding commitment to an external party. Non-compliance to internal governance processes are also captured within this report.

STRICLTY CONFIDENTIAL

POL00423569

Appendix A – All Open Material Incidents

Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Risk Rating	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
23/03/2017	Professional Services	HR	Lisa Cherry	Various	£ 800,000		In flight	PCR OJEU level	Requirements and HR personnel changed. OLD PSL fell into disuse.
10/01/2018	IT Software	Retail & Franchise	Amanda Jones (interim)	NCR	£ 1,800,000	Low	Pending	PCR OJEU level	Annual maintenance and support provided under Regulation 32 exemption for IPR. Tender planned for new systems/software in 2020/21 subject to funding.
23/04/2018	Marketing	Marketing & Brand	Emma Springham	CACI	£ 600,000	Medium	Pending	Medium threshold	Was a previous compliant contract - now extended non compliantly .
19/10/2018	Identity Services	Identity Services	Owen Woodley	Digidentity Services	£ 920,000		Pending	PCR OJEU level	Variation to non compliant contract to reduce charges following UK Verify changes
18/12/2018	IT Software	Financial Services	Owen Woodley	Space Between	£ 250,500	Low	In flight	Medium threshold	CRO Optimisation Services on POL website which have organically grown in value over time. Compliant process has now been run with service transitioning to new provider in April 2020 subject to contract. Interim extension entered into in February to provide services until a cutover can be completed.
04/01/2019	Digital Services	Financial Services	Owen Woodley	Webhelp	£ 321,000	Low	In flight	PCR OJEU level	Current contract expired 14/12/18. Retrospective extension was prepared but not executed (to 31/12/19). Services have now ceased with full and final settlement letter to be drafted with legal for Services to 06/01/20. There have been no final costs/claims yet submitted by WebHelp (29/04/20) so POL has not been able to confirm "full and final settlement" letter.
05/03/2019	Marketing	Marketing & Brand	Amanda Jones (interim)	Two Visual	£ 50,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
27/03/2019	Goods for Resale	Retail & Franchise	Owen Woodley	Vow Retail Ltd	£ -	Low	In flight	Lower threshold (PCR not applicable)	INCOME £450: Contracts for wholesale and online channels were renewed under existing existing contracts which were advertised under PCR and without stand alone contracts being put in place (this action would bring them into compliance as neither fall inder CCR or PCR).
15/06/2019	Marketing	Marketing & Brand	Emma Springham	RAPP/ CODE	£ 1,000,000	High	In flight	PCR OJEU level	OJEU expired
14/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 2,000,000	Low	None	PCR OJEU level	Business Preference. Contract and internal governance retrospectively completed.
28/11/2019	Management consultancy	Finance	Nick Read	McKinsey	£ 250,000	Low	None	PCR OJEU level	Business Preference. Contract and internal governance retrospectively completed.
23/12/2019	PR	Corporate Affairs & Comms	Nick Read	Cardew Group	£ 127,000	Medium	None	Medium threshold	GLO Response. Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	Abcomm	£ 42,000	Medium	None	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.

STRICLTY CONFIDENTIAL

POL00423569

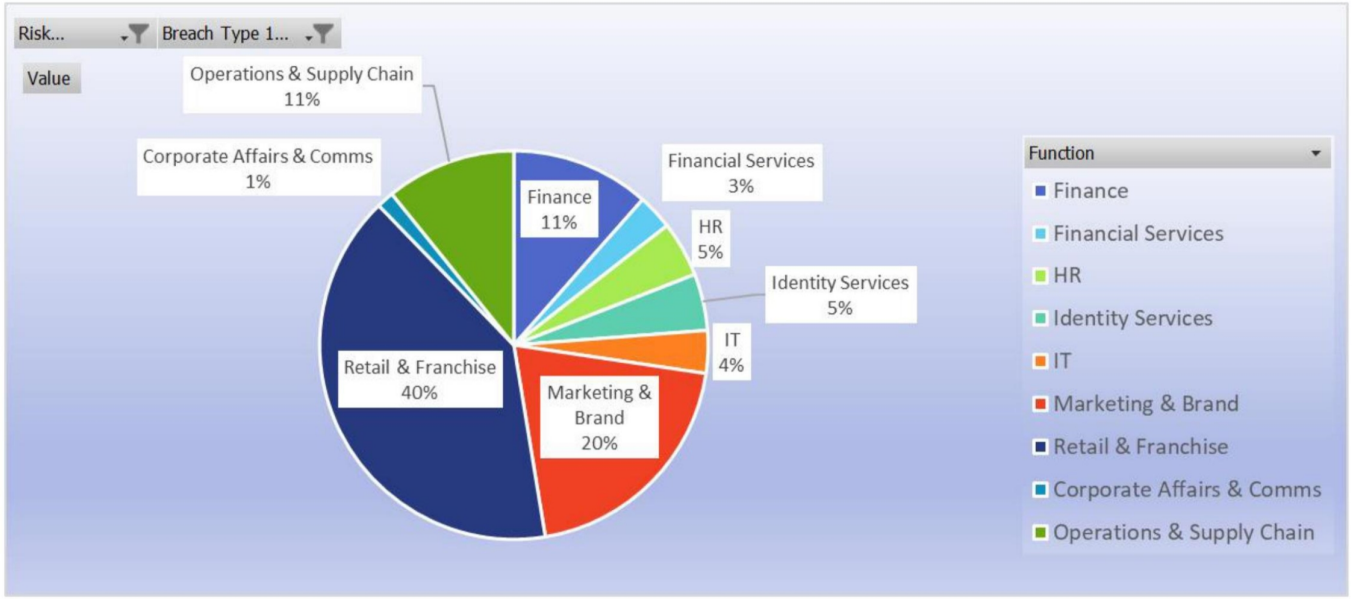
Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Risk Rating	Mitigation	Breach Type 1 - PCR Threshold	Reason for Breach
30/12/2019	Digital Services	Retail & Franchise	Amanda Jones (interim)	9XB	£ 30,000	Medium	None	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Comms, R&I & PR	Corporate Affairs & Comms	Richard Taylor	Kantar	£ 52,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
30/12/2019	Market Research	Corporate Affairs & Comms	Richard Taylor	AB Publishing	£ 100,000	Low	Pending	Medium threshold	Business Preference. Contract and internal governance retrospectively completed.
27/03/2020	IT Software	IT	Jeff Smyth (interim)	Interchange	£ 292,995	Low	Pending	PCR OJEU level	POL inherited the Galaxy system and support contracts from Royal Mail was part of, then descoped from compliant OJEU tender for Back Office in 2015
29/03/2020	IT Software	IT	Jeff Smyth (interim)	CSM Accent	£ 30,000	Low	Pending	Medium threshold	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	IT Software	IT	Jeff Smyth (interim)	JDW	£ 169,000	Low	Pending	Medium threshold	Part of the Galaxy solution for Swindon stocks, the future of Swindon has been under consideration for sometime and these licenses and support contracts have been rolled over year on year in the absence of a long term direction
29/03/2020	Media	Marketing & Brand	Emma Springham	Carat	£ 1,873,000	Low	In flight	PCR OJEU level	Contract extended to cover OJEU process time line which has been extended . Approved by Board March 2020
29/03/2020	Marketing	Marketing & Brand	Emma Springham	CACI	£ 392,380	Low	None	PCR OJEU level	No frameworks and no appetite in business for full OJEU. Limited other suppliers who have access to the market or simillar software. Software Reseller not an option. Approved by Board March 2020
29/03/2020	Banking Services	Operations & Supply Chain	Alisdair Cameron	RBS	£ -	Low	In flight	Lower threshold (PCR not applicable)	Covid19 crisis - cash services. Approved by Board March 2020
01/04/2020	Occupational Health	HR	Alisdair Cameron	Optima	£ 100,000	Low	In flight	PCR OJEU level	Interim extension to rectify CCS Framework legal drafting fault on GDPR. Approved by Board March 2020
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley	Vow Retail Ltd	£ -	Low	In flight	Lower threshold (PCR not applicable)	Compliant standalone agreements not completed by 31/03/20. Approved by Board March 2020
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley	Global Payments	£ 6,000,000	Low	In flight	PCR OJEU level	Interim extension to allow CCS tender process to be run. CCS Framework 9 months late to market on a rolling 2 month notice. Approved by Board March 2020
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	SMI	£ 175,106	Low	None	Medium threshold	Covid19 crisis . Approved by Board March 2020
30/04/2020	Management consultancy	IT	Jeff Smyth (interim)	McKinsey	£ 400,000	Low	None	PCR OJEU level	Strategic review of Horizon system options. Approved at March 2020 Board
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	Pink Office	£ 1,739,880	High	In flight	PCR OJEU level	Covid19 crisis . Approved by Board March 2020
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron	Fluid Branding	£ 195,450	Low	In flight	PCR OJEU level	Covid19 crisis . Approved by Board March 2020

STRICLTY CONFIDENTIAL

POL00423569

Appendix B – Breakdown of Open Non-Compliant Risk by £/Vol./Owner

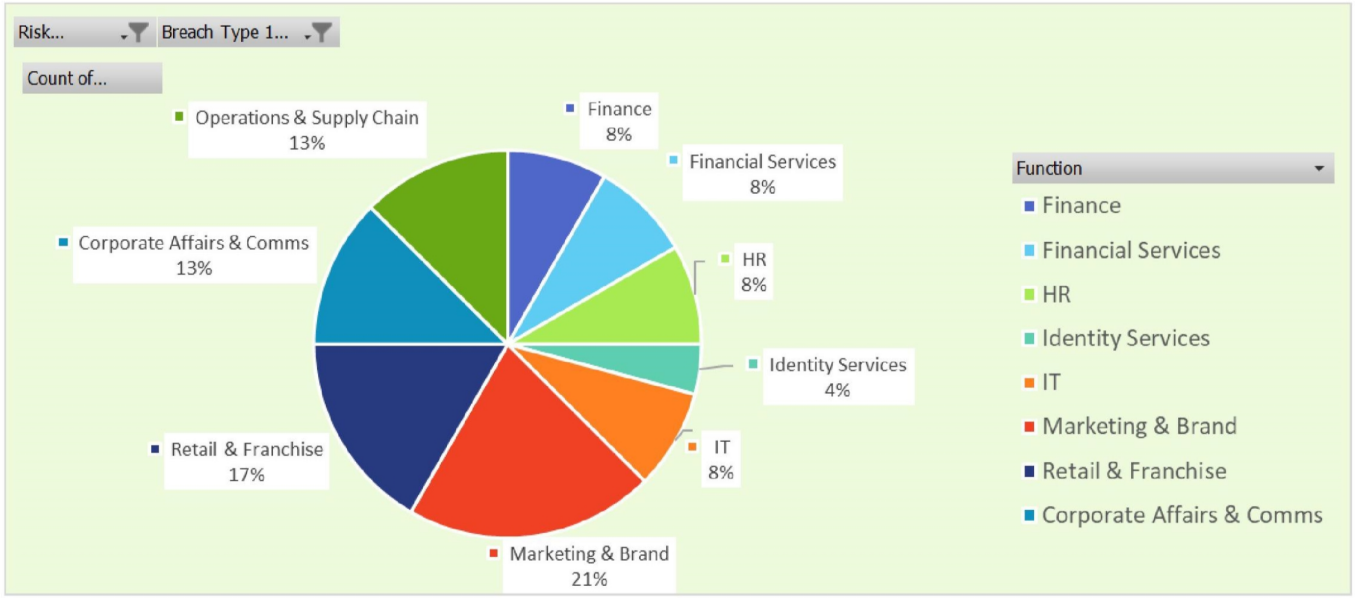
Row Labels	Sum of Value/	
Alisdair Cameron	£	2,210,436.00
Nick Read	£	2,377,000.00
Owen Woodley	£	7,491,500.00
Lisa Cherry	£	800,000.00
Emma Springham	£	3,865,380.00
Amanda Jones (interim)	£	1,922,000.00
Richard Taylor	£	152,000.00
Jeff Smyth (interim)	£	692,995.00
Grand Total	**£**	**19,511,311.00**



STRICLTY CONFIDENTIAL

POL00423569

Row Labels	Count of Value/Income
Finance	2
Financial Services	2
HR	2
Identity Services	1
IT	2
Marketing & Brand	5
Retail & Franchise	4
Corporate Affairs & Comms	3
Operations & Supply Chain	3
Grand Total	**24**



STRICLTY CONFIDENTIAL

POL00423569

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE REPORT

Title:	Criminal Misconduct and Cooperation with Law Enforcement Agencies	**Meeting Date:**	6 May 2020
Author:	Rodric Williams, Head of Legal (Dispute Resolution) Hannah Laming, Peters & Peters	**Sponsor:**	Ben Foat, Group General Counsel

The RCC is asked to:

1. **APPROVE for submission to the Audit, Risk & Compliance Committee (ARC)** the proposed "Group Policy: Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct" (the "Draft Policy"; Appendix 1), which promotes a risk-based approach to law enforcement cooperation.

   In order to approve the Draft Policy, the RCC is also asked to:

2. **DECIDE** whether POL's policy will be to cooperate with mandatory requirements and voluntary requests by law enforcement agencies where the risk to undermining the integrity of HNGA is low or low/medium;
3. **APPROVE** with respect to the Tools supporting the Policy:
   a. the process for determining what information can be provided to law enforcement agencies for intelligence purposes (Tool 1);
   b. the process for determining when evidence can be provided to law enforcement agencies (Tool 2); and
   c. the process for proactively disclosing to law enforcement agencies disclosable material in criminal cases where Horizon-derived data is being used (Tool 4);
4. **DECIDE** whether POL's policy should be not to conduct any private prosecutions at present; and
5. **DECIDE** whether Post Office should report internal criminal misconduct to the police and ask Post Office operators to advise Post Office if they make a victim crime report;

   for onward submission to the ARC.

Previous Governance Oversight

The Draft Policy has been prepared with assistance from specialist criminal law solicitors Peters & Peters Solicitors LLP ("P&P") and input from Operations, Security, and Compliance teams including Financial Crime and Information Rights.

POL00423569

Executive Summary

Post Office is a limited company owned by the Government and consequently it is important that it protects public monies and adheres to appropriate business practices and lawful requirements. The Draft Policy has been prepared to set the operating standards relating to Post Office's management of suspected criminal misconduct within the organisation and cooperation with Law Enforcement Agencies.

The Draft Policy specifically seeks to balance the risk that the reliability of Horizon, in particular the HNG-A version currently in use, is put in issue in criminal court proceedings to which Post Office is not a party (the findings of which could adversely impact Post Office's operations), against the risks that arise if Post Office does not provide or unnecessarily limits assistance to law enforcement agencies when criminal misconduct is suspected.

The Draft Policy does so by implementing a risk-based approach to the provision of information and evidence deriving from Horizon. The aim is to ensure that the findings in the Horizon Issues Judgment are drawn to the attention of law enforcement agencies as appropriate when information deriving from Horizon is provided on an intelligence basis and, where any evidence is to be provided that presents a medium or high risk in terms of the possibility of adverse findings in the future, this is escalated for risk assessment and appropriate mitigation in accordance with the Tools supporting the Draft Policy.

The Draft Policy also addresses the risks that arise from Post Office continuing to conduct its own criminal investigations and private prosecutions by precluding this activity for the time being.

9

Questions addressed

1. Why is the Draft Policy necessary?
2. What are the key risks the Draft Policy seeks to address?
3. What is the current position regarding Horizon's reliability?
4. What are the risks and impact of a judicial finding or comment in relation to the reliability of HNG-A against the risks and impact of Post Office refusing voluntarily to provide Horizon data to law enforcement agencies?
5. How does the Draft Policy work in practice, including in relation to: (i) private prosecutions; (ii) providing information or evidence to law enforcement agencies in respect of criminal investigations and prosecutions; and (iii) Post Office or postmasters making Victim Crime Reports to the police.

POL00423569

Report

Q1. Why is this Policy necessary?

1. Historically, Post Office has conducted numerous criminal investigations and brought private prosecutions in cases where it suspects that it (or its operators) have been the victim of criminal misconduct by Post Office employees or operators. In recent years, it has almost entirely stopped doing so and, since January 2015, Post Office has only bought three private prosecutions.[1]

2. In addition, Post Office regularly provides wide-ranging assistance to the police and other law enforcement agencies.[2]

3. In light of the "Horizons Issues Judgment" given in the Post Office Group Litigation and the Criminal Cases Review Commission's ("CCRC") referral of (at least) 39 past prosecutions to the Court of Appeal ("the CCRC Referrals"), these activities now give rise to the key risks identified below, all of which could give rise to significant reputational harm and/or result in financial damage to Post Office.

4. The critical risk, of most concern to the business is that the provision of Horizon-derived data to law enforcement agencies could result in the integrity and credibility of the current Horizon system (HNG-A) being unreasonably undermined in the course of criminal proceedings (e.g. because a court finding is made on an incomplete picture). This could bring Post Office's entire operating system into disrepute, thereby causing a material business continuity issue.

5. Post Office is subject to various legal duties which oblige it to provide Horizon-derived data to law enforcement as part of BAU activity. The Draft Policy ensures that Post Office continues to comply with those duties. Where no such legal duty arises, it will still generally be in the public or Post Office's interests to provide Horizon data proactively or on request, but in limited circumstances, Post Office has determined that legal, operational and reputational risks outweigh these interests. These risks arise most acutely when Post Office is asked to provide evidence, i.e. formal statements for use in court proceedings, as opposed to data on an "intelligence-only" basis.

6. The Draft Policy's objective is to enable the careful management of the risks that arise from the provision of Horizon-derived data by implementing a risk-based approach to assisting law enforcement as outlined in the Draft Policy and supporting Tools. This would enable Post Office to respond to the majority of requests for assistance from law enforcement agencies with minimal risk and disruption to business, whilst ensuring that appropriate escalation, scrutiny and management apply to higher-risk cases.

7. In addition, the Draft Policy directs that Post Office will no longer conduct private prosecutions. This is to avoid the risk that Post Office is subject to the same or similar criticisms as those levelled against it in the current CCRC Referrals, with the consequent litigation, financial and reputational risks. Where suspected criminal misconduct is identified which Post Office might historically have prosecuted itself, Post Office will consider making Victim Crime Reports to the police as appropriate.

9

[1] These prosecutions are briefly summarised in para.26 below.
[2] In this context law enforcement agencies includes any agency able to conduct criminal investigations or bring prosecutions, e.g. the police, National Crime Agency ("the NCA"), HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, OfCom and the Information Commissioner's Office.

POL00423569

8. The RCC is asked, subject to consideration of the issues discussed further in this report, to **APPROVE** taking the Draft Policy forward for consideration by the ARC.

Q2. What are the key risks the Draft Policy seeks to address?

9. The key risks the Draft Policy seeks to address are:

   a. If a court makes adverse findings about the reliability of the current Horizon system (HNG-A), this could undermine POL's ability to rely upon the Horizon system and have very serious operational implications for Post Office's business continuity;
   b. A blanket refusal to provide voluntary assistance to Law Enforcement Agencies where data derives from Horizon might result in reputational harm to Post Office and, in the case of regulators, may undermine their confidence in Post Office's ability to conduct regulated activities if they cannot vouch for the reliability of Horizon;
   c. That data deriving from Horizon is provided to law enforcement agencies and ultimately relied upon as evidence in circumstances where it is unreliable, which may result in adverse findings about Horizon data and/or against Post Office employees, could result in miscarriages of justice, and could cause reputational and financial harm to Post Office;
   d. Private prosecutions conducted by Post Office are subject to legal challenge on the basis that the investigative or prosecutorial process constitutes an abuse of process (for the same or similar reasons to those forming the basis of the CCRC Referrals), resulting in reputational and financial harm to Post Office.

Q3. What is the current position regarding Horizon's reliability?

9

10. In the Horizon Issues Judgement, Fraser J considered the Horizon system used by Post Office between 2000 and 2018. In his judgment he found (amongst other things) that it was possible for bugs, errors or defects in the Horizon system to have the potential to cause discrepancies or shortfalls in a subpostmasters' branch accounts or transactions, and also to undermine the reliability of Horizon to accurately process and record transactions. He further found that this had happened on numerous occasions and that subpostmasters were not alerted to such bugs, errors or defects.

11. Fraser J's findings as to reliability can be summarised by reference to the three versions of Horizon in use between 2000-2018:
   a. Legacy Horizon (2000 to 2010) and HNG-X (2010 to 2017/8) were not reliable and the issues identified with Horizon could have caused discrepancies in branch accounts and undermined the reliability of Horizon to accurately process and record transactions;
   b. HNG-A (currently in use following a staged roll out across Post Office's branches which took place between approximately February 2017 and November 2018) is "relatively robust";
   c. The findings in the judgment apply to Horizon historically and do not apply to HNG-A as at 16 December 2019 (the date of the judgment).[3]

[3] It should be noted that the Historic Shortfall Scheme established following the settlement of the Group Litigation excludes claims relating to HNG-A relying on Fraser J's findings in the Horizon Issues Judgment.

POL00423569

12. Fraser J's adverse findings go primarily to the reliability of data deriving from historic Horizon systems, rather than the current HNG-A system. Post Office does not have any reason at present to believe that data deriving from HNG-A is inherently unreliable, but it is important for Post Office to be alive to the possibility that such issues might arise or come to light in the future and ensure that any issues are escalated appropriately and investigated.

Q4. What are the risks and impact of a judicial finding or comment in relation to the reliability of HNG-A against the risks and impact of Post Office refusing voluntarily to provide Horizon data to law enforcement agencies?

13. If HNG-A's reliability were to be reasonably undermined in the course of criminal proceedings, this could bring Post Office's entire current operating system into disrepute, thereby causing a material business continuity issue.

14. The potential impact of this risk if it materialised is **very high** as it could cause Post Office's entire business to fail, if, as a result of a judicial finding, it was unable to rely on HNG-A in its normal business activities.

15. An adverse finding by a court, in the criminal context, is most likely to arise where Post Office has provided data or information deriving from HNG-A as evidence (i.e. by way of a formal witness statement and exhibits, not simply on an intelligence-only basis). This is most likely to arise where a defendant applies to exclude Horizon data either as inherently unreliable or on the basis that it would unfairly prejudice the proceedings. Regardless of the legal determination, the potential reputational damage of media reports of such proceedings would undermine the confidence in the system.

16. These risks have to be weighed against the risks of refusing to cooperate with law enforcement agencies and, conversely, the benefits to Post Office of such cooperation, as well as the risk of regulatory and/or audit scrutiny if Post Office take steps that imply (without justification) that HNG-A is unreliable.

17. In certain circumstances, Post Office is legally obliged to provide information and assistance to law enforcement agencies, e.g. the obligation to submit Suspicious Activity Reports ("SARs") to the National Crime Agency where money laundering or terrorist financing offences are suspected. The Draft Policy ensures that Post Office continues to comply with those duties.

18. Even where there is no legal obligation to provide information, there is generally a significant public interest in supporting the prevention, detection and deterrence of criminal misconduct.

19. There is a risk therefore that Post Office will suffer significant reputational damage if it does not assist law enforcement agencies, especially if Post Office's customers, trading partners and shareholder stakeholders expect it to provide such assistance. The impact of the Draft Policy if implemented may be that the police are unable to proceed with investigations and/or prosecutions of criminal misconduct in the absence of cooperation from Post Office.

POL00423569

20. Furthermore, failing to maintain a good relationship with the police, Crown Prosecution Service, National Crime Agency etc. could make them reluctant to address criminal misconduct where Post Office, its operators or customers are the victims of crime. It may also undermine Post Office's ability to be involved in groups and initiatives whose objective is to prevent crime and facilitate its investigation, for example the Joint Money Laundering Intelligence Task Force.[4]

21. Similar considerations apply to Post Office's cooperation with its regulators. Were Post Office to refuse to provide information to one of its regulators or provide it with a caveat that it may not be reliable, consistently or over a significant period, then there is a risk that the regulator will make its own inquiries or conduct its own investigations (e.g. into the reliability of HNG-A and supporting processes) and, in the worst case scenario, may challenge whether Post Office should be permitted to conduct regulated activities unless/until any issues are resolved. Similar risks arise if a regulator learned that, in certain circumstances, Post Office did not consider its own data to be sufficiently robust to be used in criminal proceedings.

22. These issues may also be relevant in the context of Post Office's relationship with its auditors.

23. In order to balance the risks discussed above, the Draft Policy permits the provision of information and evidence to law enforcement agencies:

a. where information is provided for intelligence-only purposes;
b. where information or evidence is provided in accordance with mandatory legal requirements or a voluntary basis with approval for the Board in higher risk situations; and
c. on a voluntary basis in circumstances without the approval of the Board where the risk of adverse findings in relation to the integrity of HNG-A is low to medium-low.

9

Q5. How does the Draft Policy work in practice, including in relation to: (i) private prosecutions; (ii) providing information or evidence to law enforcement agencies in respect of criminal investigations and prosecutions; and (iii) Post Office or postmasters making Victim Crime Reports to the police.

Private Prosecutions

24. Historically, Post Office has brought many private prosecutions (i.e. where Post Office conducts the criminal investigation and prosecution itself, rather than this being undertaken by a public body).

25. Post Office has no special power to bring private prosecutions; it brings them pursuant to s.6(1) of the Prosecution of Offences Act 1985, which enables any individual or corporate to bring private prosecutions. Despite having the ability to do so, most corporations do not bring private prosecutions where they suspect that criminal misconduct has occurred, rather they refer such cases to the appropriate law enforcement agency.

[4] JMLIT is a partnership between law enforcement and the financial sector to exchange and analyse information relating to money laundering and wider economic threats. Post Office is currently a member of JMLIT.

POL00423569

26. Since January 2015, Post Office has only conducted three prosecutions on its own behalf. Those private prosecutions can be summarised as follows:
    a. IRRELEVANT – a branch assistant who pleaded guilty on 5 November 2015 to three charges of theft from elderly customers by taking over their accounts;
    b. IRRELEVANT – postmasters who both pleaded guilty to theft on 22 January 2015. This related to a shortage identified at audit which they explained they had taken;
    c. IRRELEVANT – a non-branch, Finsbury Dials Post Office employee who pleaded guilty on or about 22 March 2019 to fraud by abuse of position relating to his abuse of postal orders, Virgin gift cards and marketing and promotion schemes.

27. The benefits of Post Office bringing private prosecutions generally include:
    a. Enabling Post Office to bring cases that the police would not accept for investigation (generally due to lack or resources and/or the cases not falling within one of their operational priorities);
    b. Successful prosecutions can be effective in deterring criminal misconduct;
    c. Successful prosecutions can help maintain the trust and confidence of Post Office's customers and the general public that their interests are being protected by Post Office.

28. The risks of Post Office bringing private prosecutions include:

    a. Reliance on Horizon data as part of the key evidence has the potential to give rise to the key risks identified above if not properly managed;
    b. To date, these risks have manifested in the GLO litigation, civil claims and consequential loss, reputational damage, as well as the extensive resource and management time spent dealing with these issues;
    c. Whilst the exact basis of the CCRC Referrals is not yet known, it is possible that the appeals will consider allegations that systemic failures in Post Office's investigation and prosecution processes rendered those cases an abuse of process. Continuing to conduct private prosecutions in such circumstances carries the risk that previous mistakes are repeated, giving rise to the same reputational and financial consequences; and
    d. There are also the operational risks to Post Office bringing private prosecutions (e.g. whether there is sufficient resource to undertake activity which had not been done for several years) and reputational risks (e.g. Post Office could be criticised for conducting new private prosecutions while its conduct of historical prosecutions is still being scrutinised through the CCRC Referrals).

29. Given the very high risk associated with bringing private prosecutions, particularly in light of the Horizon Issues Judgment and the CCRC Referrals and the fact that this is not a necessary activity because suspected criminal activity can be referred to the police for investigation, the Draft Policy directs that Post Office will not bring private prosecutions.

POL00423569

Cooperating with law enforcement agencies and providing data for intelligence or evidential purposes:

Data provided for intelligence purposes (Draft Policy Tool 1)

30. The risks associated with the provision of data to law enforcement agencies varies according to the purpose for which the data is supplied. Where the information is to be used solely for "intelligence" purposes, it will ordinarily constitute a line of enquiry to be pursued by the relevant law enforcement agency, and may not therefore ultimately end up being used in court. Whilst every endeavour should be made to ensure that the data provided is accurate, no express assurances are being given as to its accuracy or reliability. Where the police wish to put into evidence data initially provided as intelligence, they will generally ask Post Office to provide it in evidential form i.e. in a signed statement or formal exhibit.

31. As material provided for intelligence purposes will not feature in a criminal trial, the risks associated with providing it to law enforcement agencies is low. Post Office could however be criticised if it provided the data and failed to advise the law enforcement agency of any issues it knows about which could challenge that data, e.g. as identified in the Horizon Issues Judgment or CCRC referrals.

32. This risk can be mitigated by implementing Tool 1 to the Draft Policy, the *Provision of Data to Law Enforcement for Intel Purposes* flowchart. As presently drafted, Tool 1 envisages that an Advisory Notice will accompany any Horizon-derived data provided to law enforcement agencies for intelligence purposes, where that data derives from Legacy Horizon or HNG-X. As matters currently stand, the Advisory Notice is only to be provided in respect of Legacy Horizon and HNG-X data, as the findings in the Horizon Issues Judgment only apply to those historic versions of the Horizon system.

33. Given that Horizon is a live and evolving system, further issues may arise or be identified which affect the accuracy and reliability of its data. It is therefore recommended that the provision of the Advisory Notice is kept under review and is revisited should anything come to light that indicates that there may be issues with later versions of the system. This is reflected in the Draft Policy's Minimum Controls.

Data provided for evidential purposes (Draft Policy Tool 2)

34. Where information is being provided in "evidential" form (i.e. for use in court), the associated risks are significantly higher. This is because such data is intended to be relied upon in criminal proceedings and assurances are being given as to its accuracy and reliability. Post Office witnesses providing statements sign a statement of truth and may be subject to cross-examination on the accuracy and reliability of that evidence (including that obtained from Horizon). Such evidence can also be the subject of legal challenge, which may result in the court making findings as to its reliability and accuracy (which could be adverse to Post Office).

35. These risks can be managed by a requirement that all requests for evidence (save for those which are categorised as "low-risk" in accordance with Tools 1 and 2) are referred to Post Office Legal, which will consider such requests and advise whether the evidence requested can be provided. Decisions as to whether data can be provided in evidential form will be

POL00423569

made with reference to Tool 2: the *Provision of Evidence to Law Enforcement* tool. Data which is categorised as "high risk" or "medium risk" will not be provided to law enforcement agencies unless Post Office is legally compelled to provide it or the Board approves its provision. Data which is categorised as "low risk" or "medium-low risk" can be provided to law enforcement agencies on a voluntary basis without Board approval.

36. The non-provision of high or medium risk data gives rise to the following risks:

a. Certain crimes which are committed against Post Office may go unpunished, often involving many thousands of pounds;
b. Postmasters, Operators and/or counter clerks may become aware that Post Office does not support prosecutions for certain types of misconduct, thereby increasing the risk that such crime is committed against Post Office;
c. The Police may decline to share any independently sourced evidence they have which would be relevant to (and may reduce) the risk assessment Post Office has to make;
d. If a postmaster reports theft by a counter clerk and Post Office declines to provide evidence to the police to support the criminal investigation, Post Office may not be able to recover the losses from the postmaster.[5]

37. To mitigate these risks insofar as possible, Tool 2 enables evidence to be provided in such cases, should Post Office wish, with Board Approval, facilitating a case by case analysis which balances the risk of an adverse finding or comment about Horizon against those identified above.

38. By way of example, one type of criminal conduct which is frequently encountered by Post Office is theft committed by "remming out" cash on Horizon to the cash centre, where no cash is physically dispatched. In these circumstances, the Stock Unit would balance as the cash appears to be sitting in "cash in pouches" when the allegation is that it had been taken by the Operator or counter clerk. There are a number of current theft prosecutions (prosecuted by the Crown Prosecution Service) which have utilised this, with sums in excess of £100,000 being stolen from individual branches.

39. This type of case would be categorised as Medium Risk, where Horizon HNG-A data is the sole or key information going to the alleged criminality. Whilst there is no reason to believe that HNG-A data is inherently unreliable, the chances of it being challenged by the defence are increased where there is no corroborative evidence. The Draft Policy therefore restricts provision of the data unless Post Office is legally compelled to provide it or Board approval is obtained.

40. If data is sought from Legacy Horizon or HNG-X as evidence of an underlying transaction or loss, this would be categorised as High Risk given the findings in the Horizon Issues Judgment, even where there is corroborating evidence. This reflects the findings in the Horizons Issues Judgment which suggest that the Horizon data sought by way of evidence may be unreliable. Again therefore, a mandatory order or Board approval is required before this data can be provided (and it must be provided with an Advisory Notice).

Monitoring of ongoing criminal cases (Draft Policy Tool 3)

[5] The impact of the implementation of this Draft Policy on Post Office's ability to assert contractual liability and pursue civil action to recover loss is outside the scope of this paper.

POL00423569

41. Once evidence is provided to law enforcement agencies, it will be necessary for Post Office to monitor the investigation or prosecution to ensure that it is aware of any challenges made to Horizon data by the defence. This will enable Post Office to have an opportunity to mitigate any risk this presents.

42. Such monitoring can be achieved by implementing Tool 3: *Monitoring of Ongoing Criminal Cases Checklist*, which requires Post Office to liaise with the external, non-Post Office Prosecution Team (e.g. police and CPS) to obtain, so far as possible, the key information identified in that Tool. In addition, Post Office shall maintain a list of ongoing Criminal Investigations or prosecutions where Post Office or its employees or Operators are the victim. This list shall be updated with developments and a weekly report of such cases shall be provided to the General Counsel.

Disclosure Checklist (Draft Policy Tool 4)

43. An additional risk associated with the provision of Horizon-derived evidence is that the issues raised in the Horizon Issues Judgment and by the CCRC Referrals may mean that there is disclosable material in the possession of Post Office of which the external Prosecution Team may not be aware.

44. If this is not drawn to the Prosecution Team's attention and disclosed as appropriate, this could result in legal challenges that could undermine the criminal proceedings, a potentially unfair trial and/or an unsafe conviction resulting in an appeal. This risk can be mitigated by the use of Tool 4: the Disclosure Checklist, which will assist in identifying any material in the possession of Post Office which satisfies the disclosure test. Such material can subsequently be supplied to the Prosecution Team, following a review by Post Office Legal.

Post Office making a Victim Crime Report to the police

45. Where Post Office no longer conducts private prosecutions, it may consider that it appropriate to report suspected criminal misconduct to the police. The benefits of doing so include:
    a. public interest factors referred to above;
    b. operators or customers may seek (and expect) Post Office's assistance and/or support in making Victim Crime Reports;
    c. reporting criminal misconduct to the police and the risk of a police investigation and prosecution will likely deter criminality within the Post Office network.

46. The risk associated with making a Victim Crime Report is that such a report may include allegations that derive from or rely upon relevant Horizon data which may be provided in the crime report and/or be requested subsequently in evidential form. It would be unreasonable for Post Office to make an allegation of crime, but refuse to provide the evidence needed by the police to substantiate it.

47. In order to mitigate this risk, before any decision is taken to report a suspected crime, the relevant employee within Post Office who suspects criminality shall have regard to Tool 5: *Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police*. If the employee, having had regard to those factors considers that a crime

POL00423569

report should be made, they shall recommend to the General Counsel that a Victim Crime Report should be made. The General Counsel will make the final decision on whether to report suspected criminality having regard to Tool 5.

48. It is also a reality that the police do not investigate every crime reported to them owing to their own resource constraints. As such, Post Office may not wish to report all criminal misconduct, but focus on the most egregious cases, cases that have vulnerable victims and those which do not contain a medium or high risk of undermining HNGA Horizon. Tool 5 includes factors of this kind.

How would the Draft Policy work in practice?

49. Peters & Peters Solicitors LLP has attached as Appendix 2, the case of Achmore, which is a worked example of how the Draft Policy operates in practice.

Next Steps

50. It is proposed that the Draft Policy be submitted to the ARC for consideration at its meeting on 19 May 2020.

POL00423569

Appendix 1

GROUP POLICY

Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct

9

Version – V0.2

POL00423569

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. The Risk 3
1.6. Legislation 3
1.7. Industry Guidance 3
2. Risk Appetite and Minimum Control Standards 5
2.1. Risk Appetite 5
2.2. Policy Framework 5
2.3. Who must comply? 6
2.4. Minimum Control Standards 7
3. Tools & Definitions 8
3.1. Tools 8
3.2. Definitions 8
4. Where to go for help 9
4.1. Additional Policies 9
This Policy is one of a set of policies. The full set of policies can be found at: 9
https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx 9
4.2. How to raise a concern 9
4.3. Who to contact for more information 9
5. Governance 10
5.1. Governance Responsibilities 10
6. Control 11
6.1. Policy Version 11
6.2. Policy Approval 11
Company Details 11

POL00423569

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls relating to cooperation with Law Enforcement Agencies and the manner in which Post Office will address suspected criminal misconduct, including whether to conduct Criminal Investigations and Private Prosecutions. Cooperation with Law Enforcement Agencies and addressing criminal misconduct 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 cooperation with Law Enforcement Agencies and the manner in which Post Office will address suspected criminal misconduct.[6] 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[7] and other stakeholders.

1.3. Core Principles

Historically, Post Office Limited has conducted its own Criminal Investigations and Private Prosecutions; undertaken Criminal Investigations in conjunction with the police; and provided a wide range of cooperation and assistance to Law Enforcement Agencies.

In conducting these activities, Post Office Limited has relied upon data deriving in whole or in part from the Horizon computer system that is used throughout its operations. The accuracy and reliability of data deriving from historic versions of the Horizon system (known as Legacy Horizon and HNG-X (collectively "Relevant Horizon Data")) was the subject of the recent High Court case of *Bates & Ors v Post Office Ltd (No 6: Horizon Issues)* [2019] EWHC 3408. Furthermore, the Criminal Cases Review Commission ("CCRC") has recently referred the convictions of 39 individuals whose cases featured evidence derived from Relevant Horizon Data to the Court of Appeal.

In recent years, Post Office Limited has almost entirely stopped conducting its own Criminal Investigations and Private Prosecutions. It does however continue to receive a large number of requests to assist Law Enforcement Agencies in the prevention, detection, investigation and potential prosecution of alleged offences.

The governance arrangements described in this Policy are based upon the following core principles:

- Post Office is committed to supporting Law Enforcement Agencies in the prevention, detection, investigation and potential prosecution of alleged offences;

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

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

POL00423569

- Post Office Limited is committed to ensuring that prosecutions are fair and that the Prosecution Team is made aware of, and provided with Disclosable Material in its possession;
- In accordance with the above commitments, Post Office will as far as possible, cooperate with Prosecution Teams and voluntarily provide information and evidence on request;
- Post Office must, however, consider and manage the risks associated with providing such support in light of the Horizon Issues Judgment and the CCRC referrals.

1.4. Application

This Policy 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 Post Office's Risk Appetite.

In exceptional circumstances, where risk sits outside of 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 Central Risk team.

For definitions please see section 3.1.

The risk to Post Office in relation to cooperation with Law Enforcement Agencies and the manner in which it addresses suspected criminal misconduct, is reviewed by the Board annually.

1.5. The Risks

Post Office is frequently asked to provide data derived from its Horizon computer system to Law Enforcement Agencies and prosecutors for use in Criminal Investigations and prosecutions. This may arise either when Post Office is a victim of crime or when it holds data which is relevant to other suspected criminal misconduct.

The Horizon Issues Judgment raises questions about the reliability of data which is derived from Relevant Horizon Data (i.e. Legacy Horizon and HNG-X). As a result of that judgment, and the referral by the Criminal Cases Review Commission of 39 cases to the Court of Appeal on the basis that they amounted to an abuse of process, Post Office is currently under intense scrutiny in respect of cases which it has privately prosecuted in the past.

The risks which this policy is intended to address are therefore as follows:

- **A court may make or be asked to make an adverse finding against HNG-A (the current Horizon system in use), which is critical to Post Office continuing to operate**;
- An unnecessarily broad refusal to provide voluntary assistance to Law Enforcement Agencies where data derives from Horizon might result in reputational harm to Post Office and, in the case of regulators, may undermine their confidence in Post Office's ability to conduct regulated activities if they cannot vouch for the reliability of Horizon;
- Post Office might instigate or support cases in which unreliable data is served as evidence;
- Law Enforcement Agencies or Public Prosecutors might rely on Horizon data in ignorance of potential reliability issues;
- Post Office might be in possession of further information (whether derived from Horizon or not) that points towards or away from the suspect's guilt of which the Prosecution Team are unaware;

POL00423569

- Post Office witnesses might be called to give evidence and be cross-examined about Horizon reliability or related issues.

1.6. Legislation

There are a number of relevant legal and regulatory requirements which are applicable, including (but not limited to):

- Criminal Procedure and Investigations Act 1996
- Proceeds of Crime Act 2002
- Terrorism Act 2000
- The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017
- Crime and Courts Act 2013

In addition, Post Office can be legally required to provide data to relevant parties if it is served with a compulsory order from a Court or Law Enforcement Agency. For example, the police can compel Post Office to provide such material by way of a production order under Schedule 1 of the Police and Criminal Evidence Act 1984, or (if a charging decision has been made), either the prosecutor or defence counsel can apply for a witness summons under section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965 requiring an individual within Post Office to give evidence or produce a document or other item in court as evidence.

POL00423569

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 is willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[8]:

- **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 organisation
- **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 matter may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required (See section 1.4 for further details).

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review and which are relevant to this Policy. The Policy suite is designed to combat money laundering, terrorist financing, bribery, corruption and fraud and ensure adherence to relevant sanctions regimes. Post Office has also historically had policies relating to criminal investigations and prosecutions but these are not currently up-to-date or formally approved by the Board.

2.3 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees.

Where non-compliance is identified, the matter must be referred to the General Counsel. All investigations will be carried out in accordance with the Investigations Policy. Where is it identified that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

[8] The Risk appetite was agreed by the Group's Board January 2015

POL00423569

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
Adverse finding against HNG-A by a court	If HNG-A data is provided for use in criminal proceedings, there is a risk that there may be adverse findings as to the accuracy or reliability of HNG-A (the current Horizon system in use), which is critical to Post Office continuing to operate.	Preventative control: Implementation of the controls set out in this Policy to ensure, insofar as possible, that data deriving from Horizon is only relied upon in criminal proceedings where a proper risk assessment and risk mitigation exercise has been conducted by Post Office.	General Counsel	Ongoing
Regulatory concern about conduct of regulated activities if HNG-A data is inaccurate or unreliable	If Regulators (many of whom also exercise powers as Law Enforcement Agencies (e.g. FCA, PRA, Ofcom, ICO)) have reason to believe that data deriving from HNG-A is unreliable, there is a risk that the Regulator may advise Post Office that they cannot use a system that they cannot rely upon.	Preventative control: Implementation of the controls set out in this Policy would ensure that Advisory Notices are only provided in relation to HNG-A data where justified.	General Counsel	Ongoing

POL00423569

Reputational damage if Post Office refuses to provide voluntary assistance to Law Enforcement Agencies	An unnecessary refusal to provide voluntary assistance to Law Enforcement Agencies where data derives from Horizon might result in reputational harm to Post Office (including as a result of justified investigations or prosecutions being discontinued) and may result in the information being compelled in any event.	Preventative control: Implementation of the controls set out in this Policy to ensure that data deriving from Horizon is provided to Law Enforcement Agencies where it is appropriate to do so, adopting the risk-based approach set out in the Policy and supporting tools.	General Counsel	Ongoing
Conduct of Private Prosecutions	Failure to comply with duties of a private prosecutor results in a trial collapsing or an unsafe conviction which is the subject of legal challenge.	Directive Control: Post Office shall not conduct Private Prosecutions or Criminal Investigations with a view to bringing Private Prosecutions.	General Counsel	Ongoing
Law Enforcement Agency investigations and prosecutions	If, in the course of providing assistance to a Law Enforcement Agency on an intelligence-only basis, Post Office provides Relevant Horizon Data, Post Office may be criticised for failing to advise the Law Enforcement Agency of the issues identified in the Horizon Issues Judgment and arising from the CCRC Referrals	Preventative Control: Where any Law Enforcement Agency makes a request to Post Office or its employees for assistance involving the provision of information for intelligence purposes, the recipient shall comply with the "Flowchart: Provision of Data to Law Enforcement for Intel Purposes" tool (Tool 1) in determining whether/how to respond. Tool 1 provides that an Advisory Notice must be provided where data is provided that derives from Relevant Horizon Data and is not Low Risk Data.	General Counsel Group Operation Director Group Chief Information officer	

POL00423569

Law Enforcement Agency investigations and prosecutions	Where a Post Office employee provides a witness statement, they will be providing an assurance as to the accuracy of any information or data provided. Where information/data is or derives from Horizon data they may be subject to cross-examination on the accuracy and reliability of the Horizon system. This gives rise to risks that the witness may not be competent to deal with these issues and/or that there will be adverse findings about the accuracy and reliability of data deriving from Horizon and/or Post Office witnesses.	Directive Control: Where Post Office or its employees are asked or compelled to provide witness statements relating to Horizon data that is not Low Risk Data, the request must be escalated to Post Office Legal. Preventative Control: In responding to requests for the provision of evidence deriving from Horizon (i.e. a witness statement or exhibits), Post Office Legal shall comply with the "Provision of Evidence to Law Enforcement" Tool (Tool 2) in determining whether/how to respond. Preventative control: Horizon data categorised as Medium or High Risk in accordance with the "Provision of Evidence to Law Enforcement" Tool (Tool 2) shall not be provided as evidence to Law Enforcement Agencies unless pursuant to a Mandatory Notice or Order or following approval by the Board. Advisory Notices shall accompany such data in accordance with the "Provision of Evidence to Law Enforcement" Tool (Tool 2).	All Employees General Counsel General Counsel	
Law Enforcement Agency investigations and prosecutions	If Post Office becomes aware of issues with the reliability of data deriving from HNG-A and does not deal with these appropriately in the context	Detective Control: Post Office Employees must notify Post Office Legal if they become aware of issues that may undermine the reliability or accuracy of data deriving from HNG-A (or subsequent versions of Horizon).	General Counsel	

POL00423569

	of provision of information to Law Enforcement Agencies and/or the provision of evidence/disclosure in prosecutions, this could result in criticism of Post Office, as well as the issues relating to adverse findings and unsafe convictions identified above.	Preventative Control: If Post Office Legal becomes aware of issues that may undermine the reliability or accuracy of data deriving from HNG-A (or subsequent versions of Horizon) they must review this Policy and the Tools that support it (including but not limited to the wording of the Advisory Notice and the circumstances in which it is provided) to implement any such revisions as are appropriate.	General Counsel	
Provision of information or evidence to Law Enforcement Agencies	Data is provided on a voluntary basis resulting in non-compliance with other legal requirements	Preventative Control: Nothing in this Policy or Tools shall be interpreted as permitting the voluntary disclosure of data where such provision would result in non-compliance with other legal obligations (for example, but not limited to, the Data Protection Act 2018 or the General Data Protection Regulation). Mandatory Orders must be sought if necessary to ensure the lawful provision of data.	General Counsel Group Operation Director Group Chief Information officer	
Law Enforcement Agency investigations and prosecutions	If Post Office does not monitor ongoing investigations and prosecutions by Law Enforcement Agencies, Post Office may fail to identify potential reliance on Relevant Horizon Data or challenges made to Horizon data by the defence. Post Office may therefore not	Preventative Control: Post Office shall maintain a list of ongoing Criminal Investigations where Post Office or its employees or Operators are the victim and any Public Prosecutions of which it is aware, updated with developments and shall provide a weekly report of such cases to General Counsel. Preventative Control:	Group Operation Director Group Operation Director	

POL00423569

	have an opportunity to mitigate any risk this presents.	Post Office shall liaise with the Prosecution Team to obtain, so far as possible, the information set out in the "Monitoring of Ongoing Criminal Cases Checklist" (Tool 3). Post Office shall make regular contact with the Prosecution Team to request an update in relation to any developments in the case (for example, whether the defence seeks to challenge Horizon evidence).		
Extant Law Enforcement Agency investigations and prosecutions (as of the date of the implementation of this Policy)	Post Office has already supplied evidence in a number of extant criminal investigations and prosecutions (prior to the implementation of this policy). This gives rise to the same risks identified above in relation to Horizon-derived data.	Preventative Control: Where Post Office is aware that there are live, ongoing Criminal Investigations or Public Prosecutions commenced by Law Enforcement Agencies prior to the implementation of this Policy in which evidence deriving from Relevant Horizon Data has been provided, they shall notify the Officer in the Case or the Prosecution Team of the Horizon Issues Judgment and the CCRC Referrals. Preventative Control: Post Office employees must provide Post Office Legal Team with copies of all Horizon-derived data which has been supplied to Prosecution Teams. Post Office Legal (or any Nominated Criminal Law Advisors acting on their behalf) shall review the material and provide advice as to whether it can be relied on and any steps that should be taken to mitigate the risk of legal challenge. Such review must have regard to the "Provision of Evidence to Law Enforcement Tool" (Tool 2),	General Counsel Group Operation Director General Counsel	

POL00423569

		but their decision will be dependent on the facts of the individual case		
Provision of Relevant or Disclosable Material to a Prosecution Team	In cases where Horizon data is relied upon by a Prosecution Team, the issues raised in the Horizon Issues Judgment and by the CCRC Referrals may mean that there is potentially Relevant or Disclosable Material of which the Prosecution Team may not be aware. If this is not drawn to the Prosecution Team's attention and disclosed as appropriate, this could result in legal challenges that could undermine the criminal proceedings, a potentially unfair trial and/or an unsafe conviction resulting in an appeal.	Preventative Control: Where Post Office is aware that Horizon data is relied upon in a Criminal Investigation or Public Prosecution, Post Office shall apply the "Disclosure Checklist" (Tool 4) to assist in identifying material which satisfies the Disclosure Test. Preventative Control: Where any request for Relevant Material or Disclosable Material is made by a Prosecution Team, Post Office shall have regard to the "Disclosure Checklist" tool in determining what material shall be provided. Preventative Control: Material to be disclosed will be submitted to Post Office Legal for review by them (or by any Nominated Criminal Law Advisors acting on their behalf) prior to its disclosure. They will review the adequacy of the disclosure against the "Disclosure Checklist" (Tool 4).	General Counsel Group Operation Director Group Chief Information officer General Counsel Group Operation Director Group Chief Information officer General Counsel	
Provision of Relevant or Disclosable Material to a Prosecution Team	Where material is provided to the Prosecution Team by way of disclosure, it may contain material that is sensitive, subject to Legal Professional Privilege or	Preventative Control: Material to be disclosed will be submitted to Post Office Legal for review by them (or by any Nominated Criminal Law Advisors acting on their behalf) prior to its disclosure. Post Office Legal will make the final decision on	General Counsel	

POL00423569

	include personal data that should not be disclosed.	what material shall be disclosed and on what basis.		
Making a Victim Crime Report	A Victim Crime Report submitted to the police by Post Office or one of its Employees or Operators may include allegations that derive from or rely upon Relevant Horizon Data which may be provided in the Victim Crime Report and/or requested subsequently.	Preventative Control: Where any Post Office internal investigation finds that Post Office, its Employees, Operators or Customers may have been the victim of crime, an assessment must be undertaken to determine whether to recommend to General Counsel that Post Office should make a Victim Crime Report. Such assessment shall be undertaken in accordance with the "Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police" (Tool 5). Preventative Control: General Counsel shall make the final decision on whether Post Office will make a Victim Crime Report having regard to the recommendation and the "Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police" tool. Preventative Control: Where any information deriving from Horizon is to be provided with a Victim Crime Report, it shall be provided in accordance with the "Flowchart: Provision of Data to Law Enforcement for Intel purposes" (Tool 1). Any evidence shall only be provided in accordance with the "Provision of Evidence to Law Enforcement" Tool (Tool 2).	General Counsel Group Operation Director Group Chief Information officer General Counsel General Counsel Group Operation Director Group Chief Information officer	

POL00423569

		Preventative Control: Where a Victim Crime Report is made, consideration shall be given to the Disclosure Checklist. Detective Control: Post Office Operators shall be asked to advise Post Office if they make a Victim Crime Report so that a central record can be maintained.	General Counsel Group Operation Director Group Chief Information officer Group Operation Director	
Record keeping	Information or evidence provided to a Law Enforcement Agency is not retained resulting in Post Office being unable to identify the information or evidence provided and assess the risks arising from the provision of any data deriving from Horizon.	Preventative Control: Each function shall maintain centralised records for 6 years or until the end of any criminal proceedings, whichever is the longer: 1. Of any Victim Crime Report made by Post Office to the police; 2. Of any known ongoing Criminal Investigation or prosecution arising from a Victim Crime Report or where Post Office has been asked to provide assistance; 3. Of any information, data, material or evidence (witness statements or exhibits) provided to Law Enforcement Agencies.	General Counsel Group Operation Director Group Chief Information officer	

POL00423569

Training	Breaches of the Policy occur as a result of inadequate training	Preventative Control: Training shall be provided to ensure that those to whom the Policy applies understand their obligations and how to fulfil them.	General Counsel Group Operation Director Group Chief Information officer	
Breach of legal obligations or requirements	Post Office is subject to various legal obligations relating to the provision of information and evidence to Law Enforcement Agencies. It is also subject to some legal restrictions on the dissemination of information provided. If Post office breaches these legal provisions this could result in the commission of a criminal offence or other sanctions, for example the imposition of fines.	Preventative Control: Any policies or processes devised to assist in the implementation of this Policy shall expressly state that nothing in the Policy or associated documents or guidance shall prevent Post Office or its employees from complying with legal obligations and/or the requirement to protect, to the fullest extent possible, the identity of whistleblowers.	General Counsel Group Operation Director Group Chief Information officer	
Engaging in conduct that is unlawful or contrary to public policy	The imposition of a policy preventing third parties from reporting crime would be contrary to public policy and could be unlawful.	Preventative Control: Any policies or processes devised to assist in the implementation of this Policy must not impose (or appear to impose) restrictions on the ability of third parties to report crime.	General Counsel Group Operation Director Group Chief Information officer	

POL00423569

3. Tools & Definitions

3.1. Tools

1. **Flowchart: Provision of Data to Law Enforcement for Intel Purposes**

The Provision of Data to Law Enforcement for Intel Purposes flowchart has been designed to determine the level of risk exposure and escalation required when providing data to external Law Enforcement Agencies. It sets out the process which must be followed in all cases where Post Office employees or associates are asked or compelled to provide information to Law Enforcement Agencies.

2. **Provision of Evidence to Law Enforcement**

The Provision of Evidence to Law Enforcement flowchart has been designed to assist Post Office Legal (and/or any Nominated Criminal Law Advisors acting on their behalf) to assess the risks associated with providing evidence in a particular case and to reach a risk-based determination as to whether such evidence should be provided.

3. **Monitoring of Ongoing Criminal Cases Checklist**

The Monitoring of Ongoing Investigations and Prosecutions by Law Enforcement Agencies Checklist has been designed to ensure that Post Office obtains the information it requires from Prosecution Teams to properly monitor the progress of ongoing criminal cases. This will ensure that Post Office is alerted to any issues which are raised in respect of Horizon-derived evidence.

4. **Disclosure Checklist**

The Disclosure Checklist has been designed to assist Post Office Security Team with identifying categories of material which are in Post Office's possession and which are most likely to satisfy the Disclosure Test. In every case in which Horizon-derived evidence is relied upon, the Security Team should, as a minimum, proactively consider the categories of material identified in the checklist for potential disclosure, even if such material has not been requested by the Prosecution Team.

5. **Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police**

The guidance on Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police has been designed to assist the General Counsel in making consistent decisions as to whether suspected criminal misconduct should be reported to the police. It identifies a number of factors which are relevant to determining whether it is in the public interest and/or the interests of Post Office to report the suspected misconduct

3.2 Definitions

"**Advisory Notice**" – refers to the Notice which must be sent to any Law Enforcement Agency where required by Tool 1 or Tool 2. The wording of the Advisory Notice can be found in Tool 1.

"**CCRC Referrals**" –refers to the Post Office cases which are being referred to the Court of Appeal (Criminal Division) by the Criminal Cases Review Commission ("the CCRC"). As of the date of this document, the CCRC has decided to refer for appeal the convictions of 39 Post Office applicants.

"**Criminal Investigation**" – refers to an investigation conducted to the criminal standard, for the primary purpose of ascertaining whether a person should be charged with a criminal offence.

"**Disclosable Material**" – refers to material which satisfies the Disclosure Test, i.e. it is material which might reasonably be considered capable of undermining the case for the prosecution or of assisting the case for the accused.

POL00423569

"**Disclosure Test**" – refers to the test set out in s.3 Criminal Procedure and Investigations Act 1996. Material is said to satisfy the disclosure test if it might reasonably be considered capable of undermining the case for the prosecution or of assisting the case for the accused.

"**Horizon Issues Judgement**" –refers to the judgment of Fraser J in Bates and others v POL (No.6: Horizon Issues Judgment) [2019] EWHC 3408 (QB) which concerned the operation and functionality of the Horizon computer system.

"**Law Enforcement Agencies**" –refers to any agency which is responsible for law enforcement in the United Kingdom, including (but not limited to): police forces, the National Crime Agency, Her Majesty's Revenue and Customs, Immigration Enforcement and Border Force, the Financial Conduct Authority, the Information Commissioner's Office, the Prudential Regulation Authority, and the Office of Communications (commonly known as OfCom). Where a Law Enforcement Agency also conducts regulatory (or other functions), this Policy apples to circumstances in which the body is exercising criminal law functions.

"Low Risk Data" – refers to the categories of data which have been identified in Tool 2 as being "low-risk", namely: CCTV; confirmation of a bank card number used in a particular transaction and details of a payment made using a particular bank card.

"**Mandatory Order**" – refers to an order or notice that Post Office is legally required to comply with (including, but not limited to: a witness summons or a production order).

"**Nominated Criminal Law Advisors**" – refers to external criminal legal advisors that may from time to time be appointed by Post Office Limited.

"**Operator**" – refers to Franchisees and Agents of Limited Companies who operate Post Office Limited Branches.

"**Private Prosecution**" – a prosecution brought by, or on behalf of, Post Office Limited, rather than by a Law Enforcement Agency or public prosecutor.

"**Prosecution Team**" – refers to the individuals who are responsible for the investigation and prosecution of a criminal case. This will most commonly be the police officer in charge of the investigation and the Crown Prosecution Service reviewing lawyer who has conduct of the case, but extends to any external law enforcement investigator and reviewing lawyer.

"**Public Prosecution**" – refers to a prosecution brought by a Law Enforcement Agency or public prosecutor (such as the Crown Prosecution Service).

"**Relevant Horizon Data**" – refers to Horizon data derived from Legacy Horizon or HNG-X.

"**Relevant Material**" – refers to any material that appears to have some bearing on any offence under investigation or any person being investigated or on the surrounding circumstances, unless it is incapable of having any impact on the case.

"**Victim Crime Report**" – refers to a report made by Post Office to the police when Post Office suspects that it or its Operators or customers may have been the victim of criminal misconduct connected with the Post Office.

POL00423569

4. Where to go for help

4.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found on the SharePoint Hub under Policies.

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: whistleblowing@postoffice.co.uk or by telephone on: GRO
- Alternatively staff can use the confidential Whistleblowing reporting service Ethicspoint provided by Navex Global available on GRO or secure on-line web portal: https://secure.ethicspoint.eu/domain/en/report_custom.asp?clientid=106826

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 Post Office Legal team.

9

POL00423569

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the General Counsel who is responsible for ensuring that the Compliance Director conducts an annual review of this Policy and tests compliance across the Post Office. Additionally, the General Counsel and the Compliance Director 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 Post Office's risk appetite.

POL00423569

6. Control

Date	Version	Updated by	Change Details
	0.1		Draft Version

6.1. Policy Approval

Committee	Date Approved
POL R&CC	
POMS R&CC	Delete if not needed
POL ARC	
POMS ARC	Delete if not needed

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

Policy Sponsor: [*name of policy sponsor*]

Policy Owner: [*name of the policy owner*]

Policy Author: [*name of the policy author*]

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.

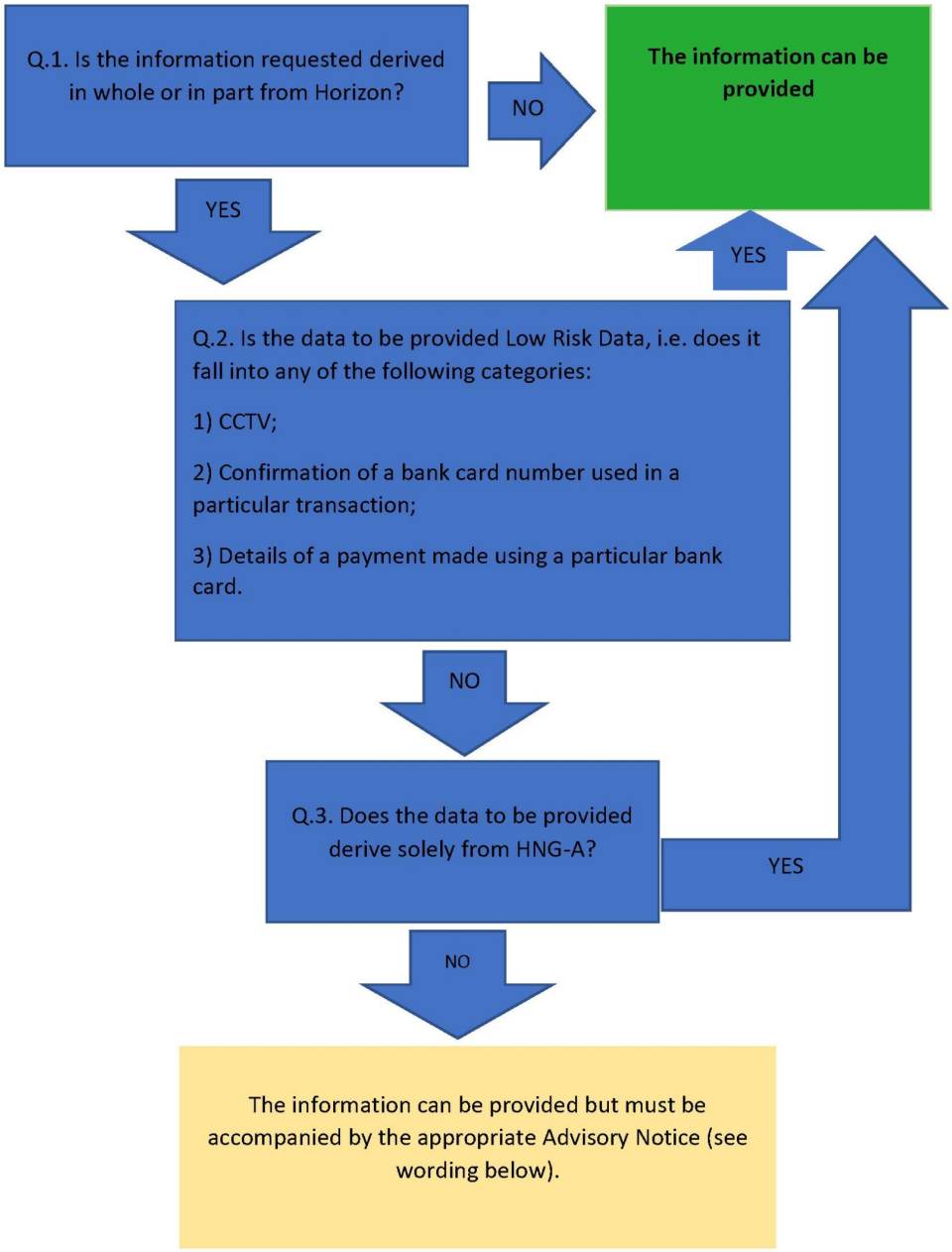
Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

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.

POL00423569

Tool 1: Flowchart: Provision of Information to Law Enforcement for Intel Purposes

1. This Tool is to be used when Post Office receives a request to provide data to law enforcement agencies for **intelligence** purposes only. If a request is made for a witness statement, or for data to be exhibited for use in evidence, please refer to Tool 2: Provision of Evidence to Law Enforcement.



9

POL00423569

2. The wording of the Advisory Notice referred to in the Chart is as follows:

"Post Office Limited wishes to assist law enforcement agencies wherever possible. However, please note that the information provided derives in whole or in part from a historic version of the Horizon computer system used by Post Office. The accuracy and reliability of data deriving from this version of Horizon was the subject of the recent High Court case of Bates & Ors v Post Office Ltd (No 6: Horizon Issues) [2019] EWHC 3408. Furthermore, the CCRC has recently referred the convictions of 39 individuals whose cases featured evidence derived from the Legacy Horizon and HNG-X systems to the Court of Appeal."

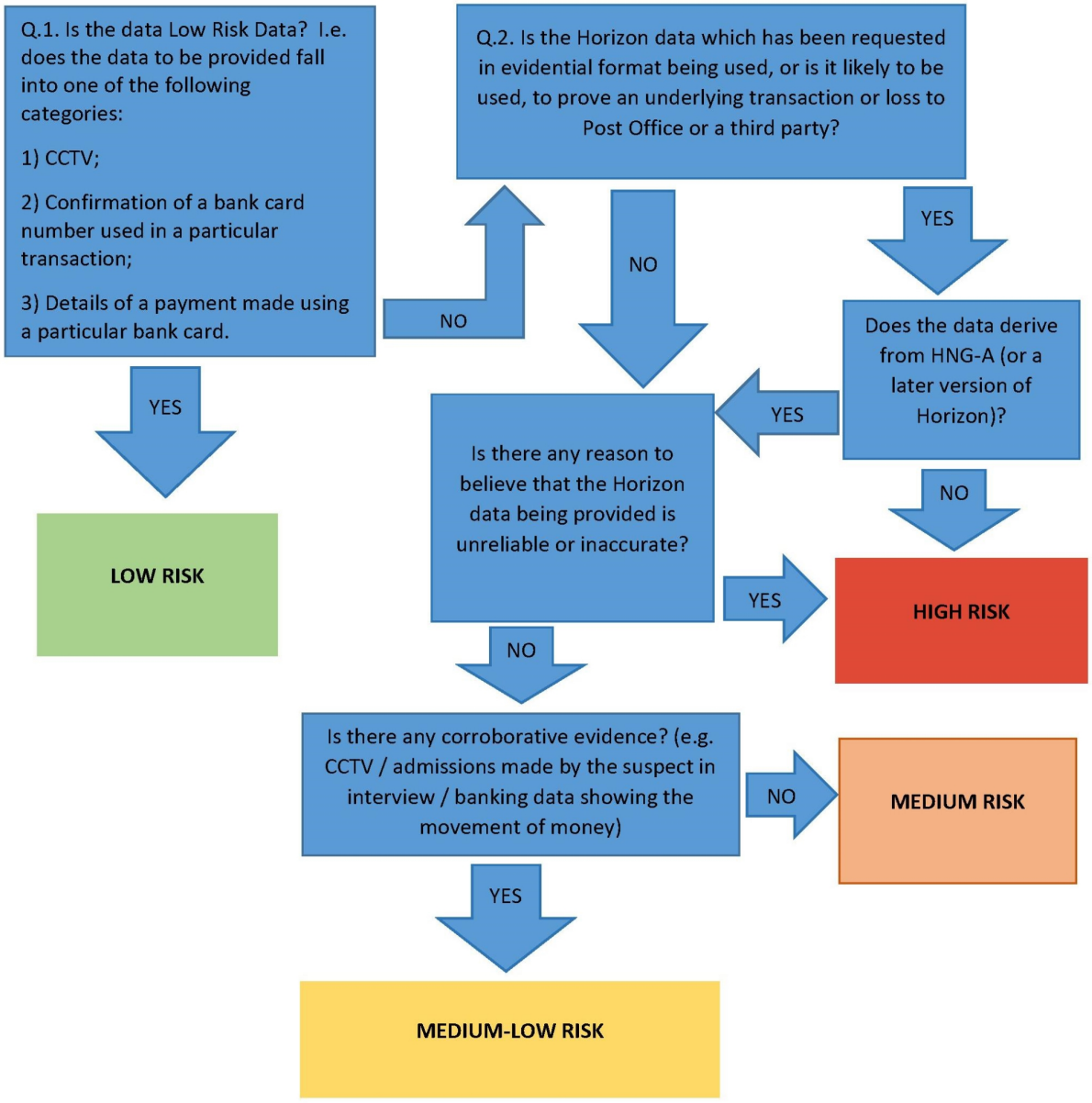
3. Nothing in this Tool shall be interpreted as permitting the voluntary disclosure of data where such provision would result in non-compliance with other legal obligations (for example, but not limited to, the Data Protection Act 2018 or the General Data Protection Regulation). Mandatory Orders must be sought if necessary to ensure the lawful provision of data.

POL00423569

Tool 2: Provision of Evidence to Law Enforcement

1. This Tool is to be read in conjunction with the Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy and will adopt the definitions therein.

2. When determining whether Horizon-derived evidence can be provided to Law Enforcement Agencies, Post Office Legal (or any Nominated Criminal Law Advisors acting on their behalf) shall have regard to the following flowchart, in order to assess the risk associated with providing the data:



9

POL00423569

3. Once the above risk assessment has taken place, Post Office Legal shall determine whether the data can be provided and any controls which are necessary to mitigate risk in accordance with the table below:

High Risk	The data **must not** be provided, unless Post Office is legally compelled to provide it or the Board approves its voluntary disclosure. If Post Office is compelled to provide the data, it must advise the Law Enforcement Agency of the risks associated with relying upon the data before providing it. If Post Office is still compelled to provide the data, the relevant witness statement **must** contain an Advisory Notice and the Disclosure Checklist (Tool 4) **must** be complied with.
Medium Risk	The data **must not** be provided, unless Post Office is legally compelled to provide it or the Board approves its voluntary disclosure. If Post Office is compelled to provide it, the Disclosure Checklist (Tool 4) **must** be complied with.
Medium- Low Risk	The data can be provided as evidence on a voluntary basis. No Advisory Notice is required. The Disclosure Checklist **must** be complied with.
Low Risk	The data can be provided as evidence and does not need to be escalated to Post Office Legal. No Advisory Notice is required.

4. Nothing in this Tool shall be interpreted as permitting the voluntary disclosure of data where such provision would result in non-compliance with other legal obligations (for example, but not limited to, the Data Protection Act 2018 or the General Data Protection Regulation). Mandatory Orders must be sought if necessary to ensure the lawful provision of data.

POL00423569

Tool 3: Monitoring of ongoing investigations and prosecutions by Law Enforcement Agencies

1. This Tool is to be read in conjunction with the Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy and will adopt the definitions therein.

2. Once Post Office becomes aware that a suspect is under investigation for a criminal offence relating to the Post Office, it shall liaise with the Prosecution Team to obtain the following information:

   a. the suspected offences or charges in each case;
   b. any information which summarises the prosecution case and defence case, however brief;
   c. procedural updates – e.g. the current stage of proceedings, next hearing date, current trial date (if applicable);
   d. whether the suspect was interviewed under caution by the police and/or Post Office investigation team and whether any admissions were made during those interviews regarding the conduct in question;
   e. whether evidence has been provided by any Post Office Employees or Operators and details of such evidence (e.g. witness statement, exhibits);
   f. whether any evidence used by the prosecution team derives from the Horizon system. If so, the nature of such evidence (e.g. evidence from Horizon transaction logs relating to spoilt label refund transactions) and the date range covered by the data;
   g. whether the suspect has raised issues regarding the veracity of the Horizon evidence or referred to the lack of training by Post Office or the possibility of remote access by Fujitsu at any stage (whether during a Post Office/police interview or a defence statement or the pre-trial stage);
   h. whether any Post Office Employee or Operator has provided any other corroborating material, other than evidence derived from Horizon system (e.g. emails, bank statements, audit reports);
   i. whether any expert reports have been provided and whether Post Office has been asked to respond to such reports.

3. If Post Office becomes aware of a challenge to data deriving from Horizon, Post Office Legal will consider any steps that should be taken to mitigate the risks arising from such challenge and may seek advice from its Nominated Criminal Law Advisors in this regard.

POL00423569

Tool 4: Disclosure Checklist

1. This Tool is to be read in conjunction with the Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy and will adopt the definitions therein.

The Checklist

2. In addition to reacting to requests for Disclosable Material made by a Prosecution Team, Post Office should be alert to the possibility that it may possess further Disclosable Material which has not been specifically requested.

3. In order to ensure that such material is not overlooked, Post Office will take a proactive approach to assisting the Prosecution Team and will draw such Disclosable Material to the attention of the Prosecution Team.

4. In every case in which Horizon-derived evidence is relied upon to prove a loss to Post Office or a third party, the person(s) conducting the review (hereinafter referred to as "the Relevant Person") must, as a minimum, proactively consider the following categories of material for potential disclosure, even if such material has not been requested by the Prosecution Team:

   a) Any calls made to any Post Office helpline (NBSC/ Horizon helpline) relating to the particular branch;
   b) Any requests made for interventions in the branch;
   c) Any requests for further training made by any staff member of the branch;
   d) Any relevant human resources records (e.g. disciplinary records of any staff member which may be relevant to the prosecution);
   e) Any audit reports demonstrating previous shortages within the branch (and the actions taken following such audits);
   f) Any material generated in contemplation of civil proceedings relating to the branch, including CIRT/SSRT Reports;
   g) Any material held by the Loss Recovery and Contracts Teams;
   h) Any further Horizon-derived data which contradicts/ undermines the prosecution case or assists the defence case.

5. Post Office should similarly have regard to the above factors prior to making a Victim Crime Report in respect of a suspected loss to Post Office or a third party.

POL00423569

6. The above list is intended to assist Post Office with identifying the categories of material which are most likely to satisfy the Disclosure Test. It is not an exhaustive list. If there is material which does not fall into any of the above categories, but which the Relevant Person considers may be Disclosable Material, this should be escalated to the Post Office Legal Team.

7. In deciding whether material satisfies the Disclosure Test, consideration should be given to, amongst other things:

    a) the use that might be made of it in cross-examination;
    b) its capacity to support submissions that could lead to:
        i. the exclusion of evidence;
        ii. a stay of proceedings (as an abuse of process), where the material is required to enable a proper application to be made;
        iii. a court or tribunal finding that any public authority had acted incompatibly with the accused's rights under the European Convention on Human Rights;
    d) its capacity to suggest an explanation or partial explanation of the accused's actions;
    e) its capacity to suggest that another individual may be responsible for the alleged offence;
    f) its capacity to suggest that an element of the offence is not made out by the prosecution;
    g) the capacity of the material to have a bearing on other evidence in the case.

6. If the Relevant Person is in any doubt about whether a particular item satisfies the disclosure test, the material should be referred to the Post Office Legal Team.

7. Any material that is identified by the Relevant Person as potentially satisfying the Disclosure Test will be provided to Post Office Legal for review. The review of material will consider:

    a) Whether it meets the test for disclosure;
    b) Whether it is subject to legal professional privilege;
    c) Whether there are any legal issues or commercial sensitivities that would arise from its disclosure;
    d) The extent to which any documents require redacting;
    e) Whether Post Office should request a notice or order compelling the provision of any of the information or material (for example because it contains personal data).

8. Post Office Legal Team may delegate any review of material to its Nominated Criminal Law Advisors as it deems appropriate.

POL00423569

9. Once the material has been subject to review, Post Office Legal Team or its Nominated Criminal Law Advisors will confirm to the Relevant Person the information and/or material to be disclosed to the Prosecution Team.

10. The Relevant Person will be responsible for making the disclosure to the Prosecution Team and for ensuring that all information and material disclosed is recorded in their Function's centralised records, together with the date and method of disclosure; the basis upon which disclosure was made (i.e. whether it was voluntary or subject to compulsion – if the latter, copies of the notice/order must also be retained); and the name(s) and contact details of the individuals to whom disclosure was made.

POL00423569

Tool 5: Factors to Consider When Determining Whether to Report Suspected Criminal Misconduct to the Police

1. This Tool is to be read in conjunction with the Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy and will adopt the definitions therein.

2. The following is a non-exhaustive list of the factors which Post Office will have regard to when determining whether it shall report suspected criminal misconduct to the police (or other Law Enforcement Agencies):

   a) Whether there is a cogent evidential basis for suspecting that a criminal offence has been committed.

   b) Whether the matter has already been reported to the police;

   c) Whether loss or harm has been suffered by Post Office Limited, POL Employees or Associates or third parties, including any financial loss or any adverse impact on Post Office Limited's business, brand, image or reputation;

   d) The extent of any actual loss or harm suffered;

   e) The extent to which Post Office relies on data deriving from Horizon, including:

      i) whether such data derives from the HNG-A system, or a historic version of the Horizon system;
      ii) whether it is relied upon to establish a loss to Post Office or a third party; and
      iii) the extent to which there are other sources of data to corroborate such loss.

   f) Whether the individual involved in the alleged criminal misconduct has repaid or offered to repay any financial loss arising from the misconduct;

   g) Whether the alleged misconduct relates to a single offence or multiple offences;

   h) The period of time over which the offending conduct has been committed;

   i) The degree of sophistication employed to commit the offence(s);

POL00423569

j) Whether there is evidence of concealment or attempted concealment by the alleged perpetrator;

k) Whether the alleged criminal misconduct involves serious or significant breaches of trust by Post Office Employees or Associates;

l) Whether the victims of the alleged criminal misconduct are vulnerable. Vulnerable victims include the elderly; those who are infirm or physically disabled; those who have mental health issues or who are less competent; and those who rely upon the state benefits system for their income.

m) The personal circumstances of the offender, for example, matters pertaining to the health or well-being of the offender or someone close to them, including any mental health issues; their age; any family or personal circumstances that are relevant to the commission of the alleged misconduct and previous good character.

n) The particular circumstances of the offence, for example, the pattern of any repeat offending; pressure to offend applied by others; force of circumstances particular to the offender or their close family, *e.g.* unequal spousal relationships, familial illness, *etc.*; a desire to assist others with no gain for the offender; or offending intended to hide personal shame or embarrassment arising out of incompetence or inability to properly fulfil duties.

o) The level of Post Office Limited resources (human and financial) involved in making a report to the police;

p) The likely deterrent effect of reporting suspected criminal misconduct.

POL00423569

Appendix 2

THE ACHMORE BRANCH INVESTIGATION

APPLICATION OF THE DRAFT POLICY: "Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct"

Introduction

1. The Achmore branch investigation can be used as a working example to demonstrate how the Policy and associated tools would operate in practice.

2. The Achmore branch investigation is an investigation being conducted by Police Scotland's Economic Crime unit. The case involves a targeted scam attack which took place between February and March 2020, whereby an unknown suspect contacted the branch purporting to be from Post Office's IT Department. The suspect requested that the elderly Operator carry out numerous deposit transactions over several days, to 'test' a problem which they had identified. The suspect had a sound working knowledge of Horizon and Post Office procedures. The total sum stolen exceeded £800,000.

3. Attempts followed at several other branches, with one additional branch being similarly duped into depositing £50,000. However, on that occasion, the bank was successful in preventing the sums from being transferred.

Assistance provided by Post Office

4. To date, Post Office has provided the police with one witness statement from the auditor, Jane Lawrence, who attended the Achmore branch after the relevant deposits had been made. The underlying Horizon data has not been supplied.

5. As the Achmore case is an extant investigation, the policy would trigger the following controls:

   i. Post Office notifying the Prosecution Team of the Horizon Issues Judgment and the CCRC referrals;

   ii. Post Office liaising with the Prosecution Team to obtain, so far as possible, the information set out in the "Monitoring of Ongoing Criminal Cases Checklist" tool and engaging in regular contact with the Prosecution Team to request an update in relation to any developments in the case;

   iii. Post Office employees providing Post Office Legal Team with copies of all Horizon-derived data which has been supplied to the Prosecution Team. This will include the statement of the auditor, as the original audit report will have relied upon Horizon Data;

   iv. Post Office Legal Team (together with P&P, if needed) reviewing the material and providing advice as to whether it can be relied upon and any steps that should be taken to mitigate the risk of legal challenge. Such review will have regard to the "Provision of Evidence to Law Enforcement" Tool (Tool 2). The Flowchart would categorise the evidence in this case to be "medium-low risk" because it is being used to prove a loss, it is derived from HNG-

POL00423569

A, there is no reason to consider that it is unreliable and there is other corroborative evidence in the case. The result of the data being classified as "medium-low" risk is that the data could be provided on a voluntary basis. No Advisory Notice would be required, but the Disclosure Checklist must be complied with.

v. Post Office including this case in its list of ongoing Criminal Investigations and Public Prosecutions of which it is aware, and providing a weekly report of such cases to the General Counsel, including any relevant developments;

vi. Post Office applying the Disclosure Checklist to assist in identifying whether there is any material in its possession which may satisfy the Disclosure Test;

vii. Any material which is considered to satisfy the Disclosure Test being referred to Post Office Legal (or any Nominated Criminal Law Advisors instructed to act on their behalf). Post Office Legal will make the final decision on what material shall be disclosed and on what basis (voluntary or subject to compulsory notice/order).

Further assistance requested by the police

6. Any further requests for assistance from the police would be addressed in accordance with Tools 3 and 4. If the police requested further intelligence from Post Office, the Policy would refer the recipient of that request to Tool 1: Flowchart: Provision of Data to Law Enforcement for Intel Purposes. As the material requested derives from HNG-A (the branch having migrated to HNG-A in 2018) and it is requested solely for intelligence purposes, at least initially, the Flowchart provides that the material **can** be supplied to the police with no further escalation to Post Office Legal Team.

7. If the police made a further request for evidence, the Policy would refer the recipient of that request to Tool 2: Provision of Evidence to Law Enforcement. Post Office Legal would make any decision to provide evidence in accordance with Tool 2: Provision of Evidence to Law Enforcement (and as set out above at paragraph 5(iv)).

Conclusion

8. In practice, the controls identified in the draft policy operate to mitigate the risks faced by Post Office in the following ways:

   i. the fact that there is a live case relying on Horizon data would be identified;
   ii. the case would be escalated for oversight and management;
   iii. the nature of the evidence relied upon would be identified and subject to a risk assessment by Post Office Legal Team;
   iv. Post Office would consider whether any proactive disclosure is needed/appropriate;
   v. Post Office Legal Team would consider the risks/benefits of providing additional evidence and whether any additional disclosure is required;
   vi. if any challenge is made to the Horizon data, this will be identified during the monitoring process.

POL00423569

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	19 May 2020
Time:	09.30 - 12.00
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Amanda Bowe (Post Office Insurance ARC Chair)
Ken McCall (SID)	Rod Williams (Head of Legal – DR & Brand) – item 4
Tom Cooper (NED, UKGI)	Ian Holloway (POI Director, Risk & Compliance) – item 6
Zarin Patel (NED)	Caroline Scott (Portfolio Director – Organisational Effectiveness): Item 7
	Martin Hopcroft (Head of Health & Safety): Item 7
Regular Attendees:	Jeff Smyth (Interim Group Chief Information Officer): Item 9.1
Tim Parker (Chairman, POL)	Tony Jowett (Chief Information Security Officer): Item 9.2
Alisdair Cameron (Group CFO)	Sherrill Taggart (Interim Legal Director) – items 10 & 11
Ben Foat (Group General Counsel)	
Andrew Paynter (Audit Partner, PwC)	
Stewart Light (Audit Director, PwC)	
Rosie Clifton (Audit Manager, PwC)	
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
David Parry (Senior Assistant Company Secretary)	

Join Microsoft Teams Meeting
GRO United Kingdom, London (Toll)
Conference ID: 690 753 133#
Pin (if applicable): 58042

10

Time		Item	Owner	Action
09.30	1.	Welcome & Conflicts of Interest	Chair	Noting
09.35	2.	Update from Subsidiaries: Post Office Management Services (ARC)	Amanda Bowe	Noting
09.40	3.	COVID-19 Response Update	Caroline Scott/ Mark Baldock/ Martin Hopcroft	Discussion & Noting
09.55	4.	Governance		
		4.1 Internal Audit Plan 2020/21	Johann Appel	Approval
		4.2 Internal Audit Charter Review	Johann Appel	Approval
		4.3 Review against Terms of Reference	David Parry	Noting
		4.4 Committee Evaluation Report	David Parry	Discussion & Noting
10.10	5.	Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy	Ben Foat / Rod Williams	Approval
10.25	6.	Previous Meetings	Chair	
		5.1 Minutes (24 March 2020)		Approval
		5.2 Action List		Noting

DRAFT

Strictly Confidential

POL00423569

POST OFFICE LIMITED

		5.3 Draft Risk and Compliance Committee Minutes (6 May 2020)		Noting
10.30	7.	Deep Dive: POI Board Risk workshop	Ian Holloway	Discussion
10.50	8.	Consolidated Report from Risk, Compliance and Internal Audit		
		8.1 Risk Report, including update on internal controls software	Mark Baldock	Noting
		8.2 Compliance Report, including the Mails Dangerous Goods Compliance Action Plan	Jonathan Hill	Noting
		8.3 Internal Audit Report	Johann Appel	Noting
11.20	9.	PCI-DSS and Cyber Security Update		Discussion
		9.1 PCI-DSS, including broader Fujitsu relationship	Jeff Smyth	
		9.2 Cyber Security	Tony Jowett	
11.35	10.	Contract Management Framework Update	Sherrill Taggart	Discussion
11.45	11.	Horizon Scanning	Sherrill Taggart	Noting
11.55	12.	Any other business	All	Noting

Next ARC Meeting: Monday 27 July 2020 at 14.30 to 17.00 in 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ

DRAFT

10

Strictly Confidential