POL00401577

POST OFFICE LIMITED

Meeting:	Audit, Risk & Compliance Committee
Date:	19 May 2020
Time:	09.30 - 12.15
Location:	1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ / Microsoft Teams

Present:	**Invited Attendees:**
Carla Stent (Chair)	Caroline Scott (Portfolio Director – Organisational Effectiveness): Item 2
Ken McCall (SID)	Martin Hopcroft (Head of Health & Safety): Item 2
Tom Cooper (NED, UKGI)	Rod Williams (Head of Legal – Dispute Resolution) – item 4
Zarin Patel (NED)	Amanda Bowe (Post Office Insurance ARC Chair) – items 6 & 7
Regular Attendees:	Ian Holloway (POI Director, Risk & Compliance) – item 7
Tim Parker (Chairman, POL)	Tom Lee (Head of Finance Financial Accounting and Controls): Item 9
Alisdair Cameron (Group CFO)	Jeff Smyth (Interim Group Chief Information Officer): Item 10.1
Ben Foat (Group General Counsel)	Tony Jowett (Chief Information Security Officer): Item 10.2
Andrew Paynter (Audit Partner, PwC)	Sherrill Taggart (Interim Legal Director) – items 11 & 12
Stewart Light (Audit Director, PwC)	Barbara Brannon (Procurement Director) – item 13
Rosie Clifton (Audit Manager, PwC)	
Johann Appel (Head of Internal Audit)	
Mark Baldock (Head of Risk)	
Jonathan Hill (Compliance Director)	
Rebecca Whibley (Assistant Company Secretary)	

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

Time		Item	Owner	Action
09.30	1.	Welcome & Conflicts of Interest	Chair	Noting
09.35	2.	COVID-19 Response Update	Caroline Scott/ Mark Baldock/ Martin Hopcroft	Discussion & Noting
09.50	3.	Governance		
		3.1 Internal Audit Plan 2020/21	Johann Appel	Approval
		3.2 Internal Audit Charter Review	Johann Appel	Approval
		3.3 Review against Terms of Reference	Rebecca Whibley	Noting
		3.4 Committee Evaluation Report	Rebecca Whibley	Discussion & Approval
10.05	4.	Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy	Ben Foat / Rod Williams	Approval
10.20	5.	Previous Meetings	Chair	
		5.1 Minutes (24 March 2020)		Approval
		5.2 Action List		Noting

Strictly Confidential

POL00401577

POST OFFICE LIMITED

		5.3 Draft Risk and Compliance Committee Minutes (6 May 2020)		Noting
10.25	6.	Update from Subsidiaries: Post Office Management Services (ARC)	Amanda Bowe	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
11.10	9.	Annual Report and Accounts & Audit Update	Andrew Paynter (PwC) Tom Lee	Noting & Discussion
11.25	10.	PCI-DSS and Cyber Security Update		Noting
		10.1 PCI-DSS, including broader Fujitsu relationship	Jeff Smyth	
		10.2 Cyber Security	Tony Jowett	
11.40	11.	Contract Management Framework Update	Sherrill Taggart	Discussion & Approval
11.50	12.	Law & Trends Update	Sherrill Taggart	Noting
12.00	13.	Supplier Contracts out of Governance	Barbara Brannon	Noting
12.10	14.	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

Strictly Confidential

POL00401577

COVID-19 Response Governance – ARC Pack

19 May 2020

Caroline Scott

POL00401577

Purpose

To ensure we:

– stay relevant to the nation and help people overcome the crisis

– make sure our Postmasters, customers and colleagues are safe

– sustain vital services with empathy

Clear programme governance to introduce good practice crisis management: a daily rhythm, meeting cadence and ways of working to support fast decision making, raising risks, issues and escalations to respond and get stuff done

POL00401577

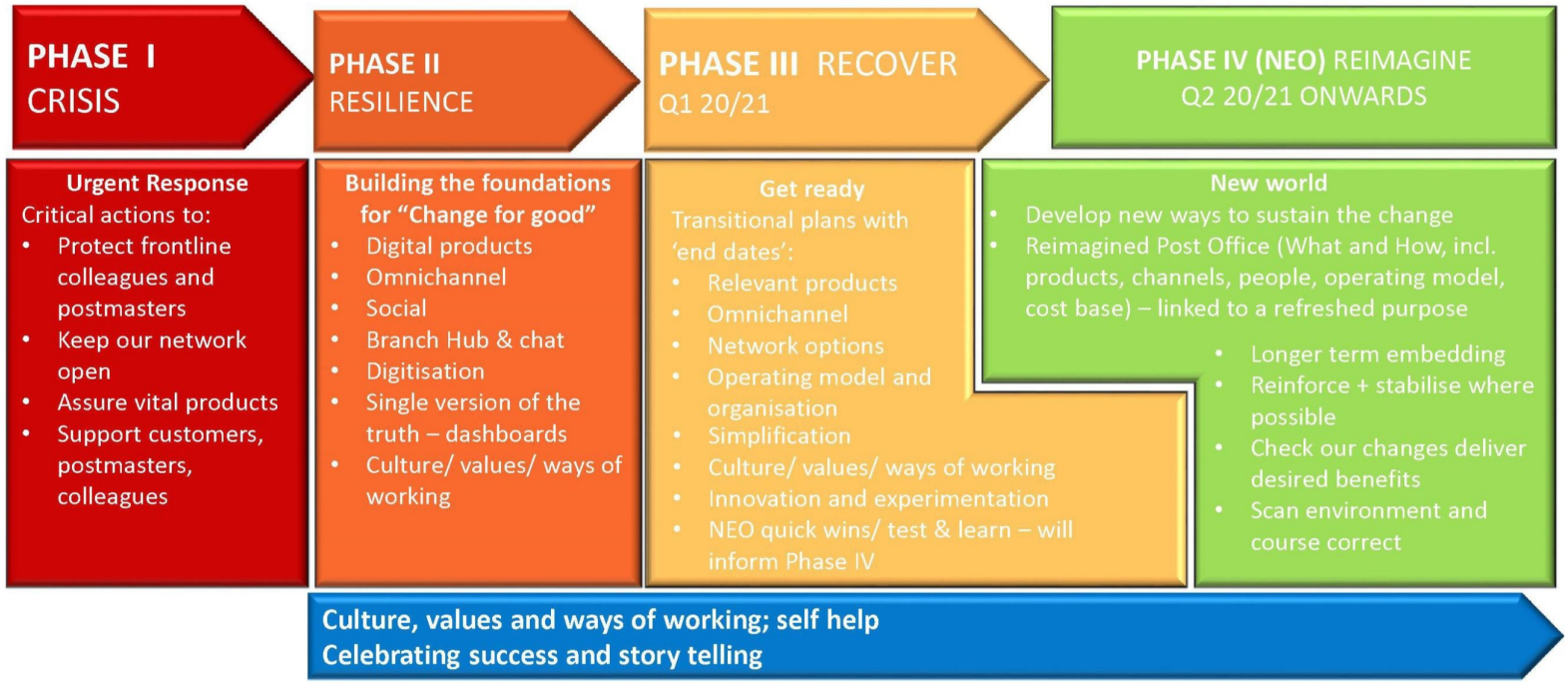
Guiding principles

- Support communities: put our customers, postmasters, colleagues at the heart of our decision making
- Protect the elderly, the vulnerable and those who are sick or dealing with bereavement
- Ensure business and team resilience to deal with mass absenteeism and provide relief
- Follow Government guidelines unless this does not make commercial sense for POL
- Apply the human touch – empathy, recognition and celebration of the small things that make a difference to our daily lives
- Recognise that actions speak louder than words to build Pride and Trust in our Post Office brand

POL00401577

COVID-19 Response Phases

– RRT and NEO: outputs will overlap as lockdown lifts in Phase III; working through principles to ensure elegant hand-offs, clarity of scope and non-duplication of projects



POL00401577

COVID-19 Risks review

Phase 1 - industry-wide and sectoral analysis of typical COVID-19 emerging risks

Phase 2 - business confirmation of relevance and assessment of *probability, likelihood* and *proximity*

Outcome:
1 single overarching COVID-19 enterprise risk
13 intermediate thematic risks (operational, strategy, legal, financial etc)
56 specific low level risks

Critical low-level risks:

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

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

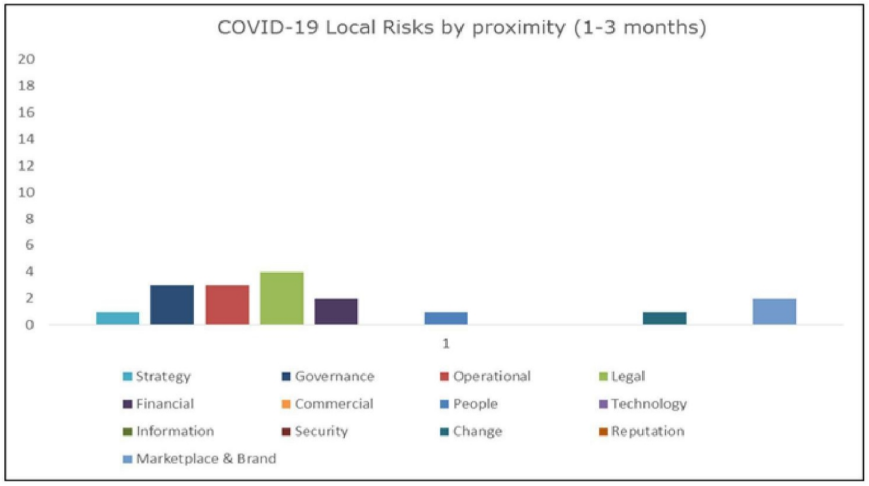
People (4:4): significant number of Post Office employees could become stressed, fearful, overwhelmed and isolated because of social distancing etc

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

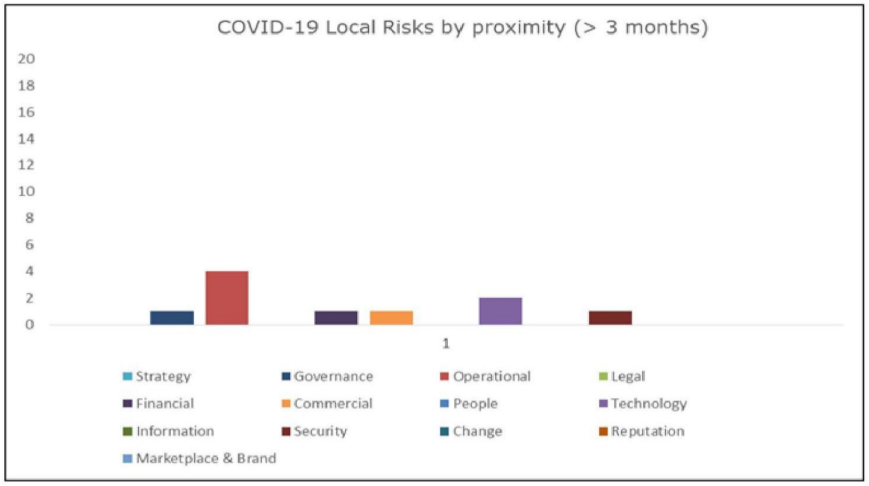
POL00401577

Risks by Proximity

- 56 specific low level risks of which 27 (50%) could materialise in the short term (within a month)
- 17 (31%) in the medium-term (within 3 months)
- 10 (19%) (over 3 months) in the long-term



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

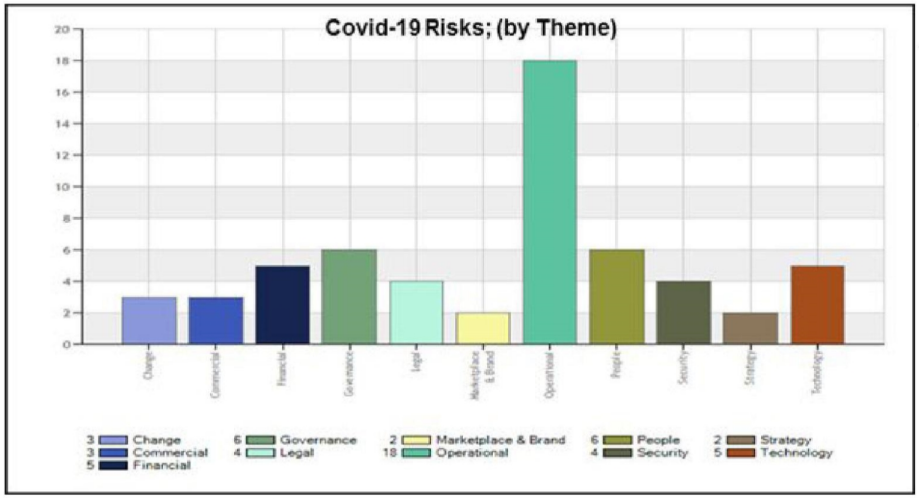


POL00401577

Medium/Long term risks

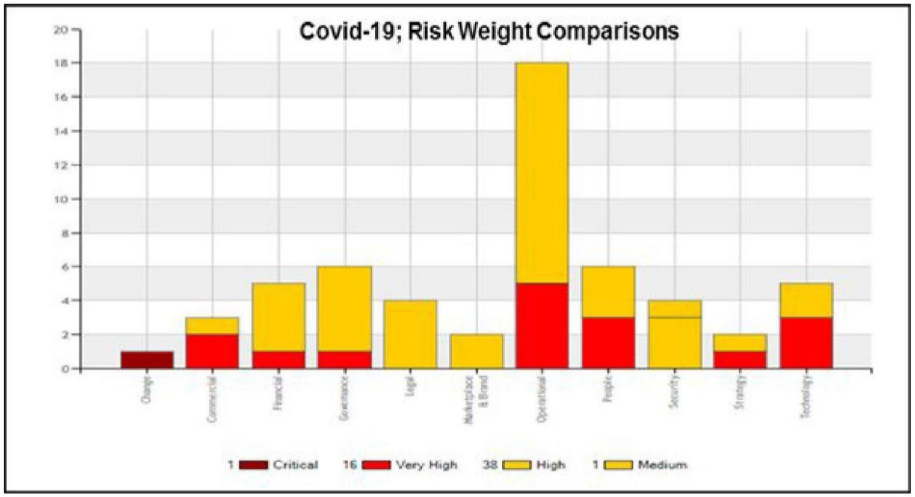
Key medium-term risks:
- **Strategy** (Unclear Target Operating Model)
- **Finance** (Cash-insufficient facility and security headroom)
- **Change** (insufficient funding)

Key long-term risks:
- **Commercial** (Long-term declining sales & demand)
- **Technology** (Failure to grasp future digitalisation opportunities)



COVID risks by theme (April 2020)

COVID risks by RAG distribution (April 2020)



POL00401577

COVID-19 Response Risks management

- COVID-19 Response has:
  - complied with business policies
  - revised them for a time limited period e.g. special leave policy revised for first 12 weeks of lockdown, or
  - consciously lightened them e.g. stage gates for increase to £45 for cashless limit

  to support the timely management of the crisis
- Simple and well communicated governance framework has been implemented, which has proved effective, including documentation of SteerCo decisions, actions, risks and mitigations
- Early Internal Audit engagement to provide for an advisory review. Interim audit report was Green
- Timely and regular access to senior stakeholders to provide direction and guidance
- COVID-19 Response team have actions in place to mitigate, reduce or manage local risks (1-3 months). Programme deliverables have been shaped by the risks which are reviewed fortnightly at SteerCo level
- Post Office, based on feedback from Risk, is ahead of the curve in comparison to other organisations

COVID-19 Response has provided the business with a head start into transformation

POL00401577

Risk mitigations/successes (1)

COVID-19 Response has some significant successes to support risk mitigations:

- **Significant remote working** – 27% of workforce (c.940 colleagues) based in all Post Office admin buildings and contact centres and all of Payzone (c.70), supported by robust technology infrastructure scaled to support accelerated adoption of technology e.g. MS Teams, or printing at home capability which was launched in 36 hrs
- **Keeping our frontline colleagues safe** - PPE has been issued to front line staff (branches and Cash in Transit) and includes screens, gloves, hand sanitiser, anti bacterial wipes, masks and order placed for face visors; social distancing materials issued to branches to advise customers
- **Call centres equipped and deployed to work at home** - including Telco and Post Office Card Account contact centres. Second Post Office Card Account contact centre stood up in 10 days and have taken 5,000 calls in their first 4 weeks (manned by Post Office and Payzone volunteers)
- **Keeping 90% of network open** – currently with c. 900 branches closed but more are reopening daily
- **Branch hub release and adoption** – opening a new and simple channel to interact with Postmasters, driving adoption with June remuneration conformance and additional functionality e.g. PPE ordering
- **Agent remuneration** - certainty provided to Postmasters regarding remuneration for April to June to encourage branches to trade and increase their opening

POL00401577

Risk mitigations/successes (2)

- **Flexibility** - for Postmaster opening hours and colleagues to work from home, enabled us to keep branches open and improved colleague productivity
- **Product innovation to support vulnerable customers** - special delivery cash service for shielding POCA customers; fast pre authorised cheque encashment; business cheque encashment; proxy agent set up by phone for POCA customers
- **Volunteering Resources** – dynamic resource pool launch; product teams and volunteers supporting social media responses (reduced response times from 1-2 days to less than 30 mins; Identify Team training to process Verify applications; volunteers offered to support cross government request
- **Maintaining our cash supply to the network** - Use of Loomis and RBS to support our supply chain operations in light of colleague absences in early weeks of lockdown
- **Dashboards** - New dashboards created to help make data based decisions and enable our teams understand where any why branches are not open
- **Legal risks** - Full contractual review undertaken to understand our risks and obligations. Training was then provided to contract owners on management of risks during these times
- **Digital Products** – products reviewed and updated to meet customers needs and enhanced with new ways to access e.g. Drop and Go application online, minimising queue time and reducing social distancing risk

POL00401577

Management of longer term risks and Next steps

- Return to workplace is being initiated under COVID-19 Response but will ensure alignment with NEO
- Close liaison with NEO team to ensure short to medium term risk mitigations do not compromise the longer term business strategy
- COVID-19 Response and Risks team 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

POL00401577

Appendix - risks

POL00401577

COVID-19 intermediate risks

R#	COVID-19 Risks	Inherent RAG	Residual RAG	Trend	Target RAG
86	**Strategy:** Risk the Post Office identifies and pursues a COVID-19 strategy which is based on flawed, inaccurate or incomplete data, cannot readily adapt to a changing macro-environment and fails to support the delivery of commitments, plans or objectives	4:2	4:2	⇨	4:1
87	**Governance:** Risk the Post Office COVID-19 Governance structure does not provide for clear plans, priorities, authorities and accountabilities and/or has ineffective or disproportionate oversight of its decision-making and/or performance	4:2	4:2	⇨	4:1
85	**Operational:** Risk that operational changes required by the COVID-19 pandemic have an adverse impact on standard operating processes resulting in fraud, error, impaired customer service, non-compliance and/or poor value for money	4:3	4:3	⇨	3:
88	**Legal:** Risk the Post Office is unable to comply with COVID-19 legislative and regulatory changes, sectoral regulator guidance and/or the outcome of other external legal activity (i.e. litigation)	4:2	4:2	⇨	3:1
89	**Finance:** Risk the Post Office is unable to manage its finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting	4:4	4:4	⇨	4:2
90	**Commercial:** Risk the Post Office is weak in the management of its commercial partnerships and contractual requirements, in COVID-19 environment, resulting in poor performance, inefficiency, poor value for money, fraud, and/or failure to meet business requirements/objectives	4:4	4:4	⇨	3:2
91	**People:** Risk the Post Office has ineffective COVID-19 leadership and engagement, suboptimal culture, inappropriate behaviours, unavailable capacity and capability, and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance	4:4	4:4	⇨	3:2
92	**Technology:** Risk the Post Office's technology does not deliver the expected COVID-19 services due to inadequate or deficient system/process development and performance or inadequate resilience	4:3	4:3	⇨	3:2
93	**Information:** Risk the Post Office is unable to produce robust, suitable and appropriate COVID-19 data/information and to exploit data/information to its full potential	4:3	4:3	⇨	4:2
94	**Security:** Risk the Post Office fails to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and GDPR non-compliance	4:3	4:3	⇨	3:1
95	**Change:** Risk the Post Office change programmes and projects are not aligned with COVID-19 priorities and so do not successfully and safely deliver requirements and intended benefits to time, cost and quality	4:4	4:3	⇨	4:2
96	**Reputation:** Risk the Post Office's reputation is damaged through COVID-19 adverse events, systemic and/or repeated failures to respond leading to destruction of trust and relations	4:3	4:3	⇨	3:2
97	**Marketplace & Brand:** Risk the demand for Post Office services and products across the various sectors declines and/or loyalty to the Brand reduces	4:2	4:2	⇨	3:1

POL00401577

COVID-19 key local-level risks

R#	COVID-19 Risks	Inherent RAG	Residual RAG	Trend[1]	Target RAG	Mitigation
46	**Change** As a result of CV19's impact on trading profit and the cost of reacting to CV19, there is a risk that there isn't enough change funding available to deliver PO's planned change activity, resulting in lost benefit, missed opportunities and fines from inability to comply with regulations	4:5	4:5	⇨	3:4	Identify projects with Regulatory impact and complete assessment as part of GE options review - end April. Continue to manage flexibility of Post Office cash flows with UKGI - [Ongoing via activity led by Finance].Continue to rigorously prioritise change activity through SPO and Investment Committee - latest version reviewed by GE on 15th April, revised 20-21 change portfolio to be agreed by GE end April and baseline plan signed off by Board in mid-May. OWNER MICHAEL BROWN[4]
31	**People** Risk that Post Office frontline staff get infected with COVID-19 by customers visiting branches to perform various counter transactions.	4:4	4:4	⇨	3:2	Provide Guidance and processes which include; Avoid close contact with the customer and keep your distance, Wipe and clean the packaging area used by customers with anti-bacterial liquid. Follow government guidelines of maintaining minimum distance (2m) between customers/staff. Perform only essential services as prescribed by the business, Use hand sanitiser after each transaction.
60	**Operational** Because of Postmaster sickness/self-isolation limiting access to a branch or because of lack of CViT resource there is a risk that it may not be possible to recover cash from individual branches for some time.	4:4	4:3	⇨	3:1	Disable Horizon in branches where cash not returned ATM funding to be limited to dispensed value in closed branches "Monitor cash flows to determine changes in branch requirements Including daily trapped cash reporting and monitoring" Contact branches by telephone to arrange collections where possible Stop cash and stock deliveries if cash not returned
51	**Operational** Because of employee or agent illness/self-isolation there is a risk branch network coverage will drop below the level needed to serve customers. If this risk materialises it could lead to customers being unable to access essential services like POCA and bill payments.	4:4	4:3	⇨	3:1	Undertake real time monitoring of closures and early identification of branches where there is a lack of alternative service provision.
29	**People** Risk that significant number of Post Office employees are stressed, fearful, overwhelmed and isolated because of social distancing, are unsure about how to remain productive while at home and are unable physically adjusted to new work schedules, locations, and routines	4:4	4:4	⇨	3:2	Deliver timely and clear communication to employees by providing clarity and curbing unnecessary fear or stress. Consider developing new policies particularly with regard to workplace disruptions caused by COVID-19. Ensure consistent policy compliance by all workers. Review existing applicable policies to ensure that they are up-to-date and identify any gaps.
26	**Commercial** Risk that Post Office short-term business-critical activities, products, services, business processes and systems have a high dependency on third parties who have a high degree of COVID-19 risk exposure	4:4	4:4	⇨	3:2	Analyse financial health and degree of Post Office reliance on critical 3rd party and advise Group Commercial. - [SMEs/Lorraine Robinson/30 April 2020] Design, agree and implement overarching prioritised action plan in light of SME analysis. - Lorraine Robinson/10 May 2020. Identify means of understanding financial health and degree of Post Office reliance on critical 3rd party. [SMEs/Lorraine Robinson/20 April 2020]
21	**Financial** Risk the Post Office will face months of exceptionally poor trading conditions with immediate lost revenue representing a permanent loss putting unanticipated pressure on liquidity.	4:4	4:4	⇨	4:2	Implement daily monitoring of cash balances Implement a cash centric culture across the business, focusing on cash, not P&L, metrics. Implement a strict 13 week cash flow forecasting process Optimize internal cash transfers. Make sure payment is performed through agreed payment method Calculate payment terms from invoice receipt date rather than invoice date. Monitor dispute resolution cycle times and address root causes Raise invoices ASAP and in a timely manner. Map business critical suppliers to determine payment priority. Review customer payment terms and identify arbitrage opportunities across customers. Implement robust payment run policy to avoid early payments

R#	COVID-19 Risks	Inherent RAG	Residual RAG	Trend	Target RAG	Mitigation
2	**Operational** Because of employee illness or need to self-isolate there is a risk that Supply Chain may be unable to provide its usual services to branches. If this risk	4:4	4:3	⇩	4:1	• Hemel FX operation repurposed to process Sterling (complete) • Contract NatWest to process up to £4m cash. Trial of 100 pouches to take place w/c 6 April.

POL00401577

	materialises it could lead to cash outs in branch and the inability to provide essential services to vulnerable customers					• Contracted with Loomis to restock ATMs if needed. Branch holdings monitored & where resource is limited branches in need of cash are prioritised to ensure branches can continue to trade. • PPE equipment provided • Enhanced clearing processes in place • Social distancing measures in place" • Coin standards removed
59	**Operational** Because trading conditions during the pandemic are likely to produce cashflow problems in many retail businesses some agents may experience cash flow and personal finance issues. leading to the risk that some Postmasters may use Post Office	4:3	4:3	⇨	3:1	New weekly monitoring of Trading Period balances settled centrally and to cash. Monitoring of recoveries will continue as normal. " Security Managers making targeted crime reduction / supportive calls to branches, specifically those who suffered a crime in the last 12 months + areas of emerging trends etc.
37	**Technology** Risk that third party suppliers are unable to source hardware to support the service due to high global demand	4:3	4:3	⇨	3:1	Ensure End of Life hardware components are prioritised Ensure process is in place to action urgent Purchase Orders process is in place to action urgent requests
36	**Technology** Risk that engineers are unable to resolve admin user issues due to working from home locations	4:3	4:3	⇨	3:2	Ensure autopilot enablement of surface pros (200) available w/c 6th April. Introduce Engineer led courier service Arrange for suppliers to send engineer direct to users home address (if no reports of virus or isolation) Build autopilot enablement that can be released to lower cost laptops that can be built off site, increasing the stock of hardware. (end of may)
34	**People** Risk that the widespread adopting of Post Office virtual workplaces could result in staff being unable to adapt to the challenge of making virtual work a meaningful experience	4:3	4:3	⇨	3:2	Dedicate time for informal and social interactions, e.g., virtual coffee sessions or team drinks. Develop practical plans to ensure the health, safety, and wellbeing of employees. Encourage cross skilling of key talent to transcend organizational and role boundaries. Institute lessons learnt sessions for teams to share learnings around new ways of work. Encourage employees to create new relationships and working
28	**Commercial** Risk the Post Office suffer long-term declining sales, reduced consumer demand, and fail to understand the impact and strategic consequences of the crisis	4:3	4:3	⇨	3:2	Actively review policies and procedures actively so they remain adaptive and flexible to long-term threats ensuring the Post Office remains prepared and protects its staff people, reputation, strategy and bottom line Consider LT Post Office commercial model (including supporting operational functions such as key systems, staff, 3rd parties etc) in light of projected post-COVID-19 macro-environment [Owen Woodley/Henk Van Hulle/15 May 2020]

R#	COVID-19 Risks	Inherent RAG	Residual RAG	Trend	Target RAG	Mitigation
13	**Governance** Risk the Post Office COVID-19 response defaults to a centralised and risk-averse approach thereby leading to bottlenecks, unnecessarily stringent governance and increased overhead for individuals and teams.	4:3	4:3	⇨	4:1	Dedicate/create new channels to share updates with staff and clearly communicate priorities Rapidly develop a COVID-19 organisational response such that official messaging is simple, honest and consistent Maintain an open door policy for staff to share honest feelings.
8	**Strategy** Risk the Post Office is unable to adapt its long-term operating model quickly and is unable to balance 'business as usual' against new COVID-19 demands and changing priorities	4:3	4:3	⇨	3:1	Undertake analysis to understand COVID-19 impact on Post Office LT business and the associated response (i.e. What should the Post Office look like following the COVID-19 crisis and what should be its essential and non-essential services
7	**Operational** Because COVID-19 is making individuals and businesses find ways of avoiding cash use (i.e. increase in contactless limit) there is a risk that there is a permanent reduction in the use of cash. If this risk materialises it could lead to a reduction in demand for Supply Chain services	4:3	4:3	⇨	3:2	Monitor cash flows to determine changes in branch requirements, including daily trapped cash reporting and monitoring Liaise with UK Finance to understand industry cashflow impacts

POL00401577

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

3.1

Title:	2020/21 Internal Audit Plan	**Meeting Date:**	19 May 2020
Author:	Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer

Input Sought: Approval

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;
- approve the re-prioritised internal audit plan for 2020/21.

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

POL00401577

Questions addressed

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

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:

POL00401577

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

POL00401577

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

POL00401577

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

POL00401577

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.

POL00401577

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

3.2

Title:	Internal Audit Charter Review	**Meeting Date:**	19 May 2020
Author:	Johann Appel: Head of Internal Audit	**Sponsor:**	Al Cameron: Chief Financial Officer

Input Sought: Approval

The committee is asked to:

- note the Internal Audit Charter, which was updated to reflect new reporting lines;
- re-approve the Internal Audit Charter for continued use for the next two years.

Previous Governance Oversight

The Internal Audit Charter was last reviewed and approved in March 2018.

Executive Summary

The Internal Audit Charter establishes the internal audit activity's position within the organisation, including the head of internal audit's (HIA) reporting lines, authorising access to records, personnel, and physical properties relevant to the performance of engagements; and also defining the scope of internal audit activities. It is therefore a reference point for measuring the effectiveness of Internal Audit.

The Institute of Internal Auditors' international standard 1000 ('Purpose, Authority and Responsibility') read together with implementation guidance 1000-1 ('Internal Audit Charter'), requires that the chief audit executive must periodically review the Internal Audit Charter and present it to senior management and the board for approval. Furthermore, par. 18(d) of the Post Office ARC Terms of Reference requires that the ARC must review and re-approve the Internal Audit Charter on a bi-annual basis.

Report

1. The Internal Audit Charter was last revised and re-approved by the ARC in March 2018.
2. The updated charter (attached as Appendix 1) was amended to reflect the new organisational structure and reporting lines. No further amendments were required to be made following this review.
3. A self-assessment performed against the charter confirmed that the requirements of the charter were complied with in all material aspects and that the charter is relevant and appropriate to continue to provide a mandate for the effective provision of internal audit services.

POL00401577

3.2

Internal Audit Charter

Internal Audit is an independent review function set up within the Post Office organisation as a service to the Board and all levels of management. The Head of Internal Audit is responsible for evidencing the effectiveness of the design and operation of all aspects of risk management and internal control frameworks throughout the organisation's activities.

Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[1]

1. Goals of Internal Audit

- Provide the Board with independent and objective assurance over Post Office Group's controls.
- Provide assurance that Post Office processes for identifying, assessing and managing risks are effectively deployed.
- To help management improve their decision making processes, controls and operations through risk and control advice and support.

2. Independence

The Head of Internal Audit will report functionally to the Chair of the Audit, Risk and Compliance Committee (ARC) who is a Non-Executive Director of the Board, and administratively on a day to day basis to the Group Chief Finance Officer. The Head of Internal Audit has access to the Board Chairman, Non-Executive Directors and the CEO. The Internal Audit staff report to the Head of Internal Audit.

3. Role and Scope

The role of Internal Audit is to understand the key risks of the organisation and to examine and evaluate the adequacy and effectiveness of the frameworks of risk management and internal control as operated by the organisation.

[1] Definition of Internal Auditing – Global Institute of Internal Auditors Inc.

POL00401577

Internal Audit, will therefore review, appraise, evidence and report on:

3.1 The adequacy and effectiveness of the frameworks of:
- Operational control across the organisation including outsourced services.
- Financial control.
- Management control.

3.2 The integrity of processes and systems, including those under development, to ensure that controls offer adequate protection against error, fraud and loss .

3.3 Company policies, (risk and non-risk) standards and procedures, including their effectiveness and appropriateness.

3.4 National and International legislation where applicable are effectively recognised and acted upon by the company.

3.5 The operation of the organisation's corporate governance and risk governance arrangements.

3.6 Significant aspects of the organisation's activity including major projects and change programmes and as directed by the ARC.

3.7 Effectiveness of the organisation's fraud management processes:

- Management remain responsible for establishing and maintaining systems for the prevention of fraud and theft. However, the internal audit department may be requested to assist in the investigation of significant suspected fraudulent activities and will notify the ARC of the results.
- Where regular audit work may reveal fraud risk or actual fraud and irregularities, this will be reported to management, the Risk and Compliance Committee (RCC) and to the ARC.

3.8 Other key stakeholders:

The Internal Audit team will liaise with other providers of assurance including second line defence functions, external audit and the Group Risk team.

4. Access and Authority

- The Post Office Internal Audit team have unrestricted access to all functions, records, property and personnel at all management levels including the external auditors and contractors insofar as it applies to authorised audits, reviews and investigations.
- All members of the Internal Audit team will abide by company and professional standards with regards to confidentiality. Audit files and evidence will be appropriately secured.
- Where information is of particular sensitivity, management may request that access to the information be restricted to the Head of Internal Audit only.

POL00401577

- If required access has not been forthcoming and following due process remains as such and this has a significant restriction on the effective completion of an audit, the limitation should be reported. Effort to resolve the situation should be undertaken and only after these steps should such limitations be reported to the Audit, Risk and Compliance Committee (ARC).

5. Reporting on activity

- The findings on engagements shall be cleared upwards through line management and to the appropriate GE member. Reports will be summarised for the RCC and ARC, who may request access to the full reports. Reports will also be provided to the CEO, CFO and other stakeholders as appropriate.
- Formal reports will be classified as confidential. Access to final reports by individuals not directly associated with the audit, shall be approved by the Head of Internal Audit and the owning GE member.

6. Audit Plan

- The Head of Internal Audit will submit a rolling risk based plan for approval by the ARC, review progress against plan with the ARC quarterly and where necessary amend the plan to reflect changing risk priorities.
- The plan will project a maximum of six to twelve months into the future although some areas will require annual review.
- The plan will also be made available to the Board and the GE and be flexible to requests from the business that arise during the year.
- Audits will generally be planned alongside management and announced, but at times visits, checks and investigations may be unannounced to the business area concerned. This includes all aspects of the group including head office functions.
- A follow-up process will be implemented. The results of follow-ups, including the implementation rate of recommendations and overdue audit actions will be reported to the ARC on a periodic basis.

7. Management Requests

Management may make requests for audits or reviews through the year:

- Requests will be evaluated in terms of risks and an effort will be made to address these requests wherever possible.
- Other than short assignments, the ARC should be informed of proposed changes to the plan especially where this will impact delivery or delay start of currently planned work.
- The Chair of the ARC and the Head of Internal Audit will discuss significant changes to the plan and agree steps with the business.

POL00401577

8. Audit Committee Liaison

- The Head of Internal Audit should meet with the Chair of the ARC outside of regular audit meetings, without the presence of management at least twice a year.
- The Head of Internal Audit may meet with any of the other members of the ARC and with the external audit partner outside of ARC committee meetings.
- All members of the committee may request a meeting with the Head of Internal Audit to discuss risk, control and audit matters.
- The Head of Internal Audit will provide support and guidance where requested to help the ARC committee members discharge their duties.

9. Staffing and Resource

- The Head of Audit shall ensure that the department is sufficiently resourced to carry out its duties in terms of professional competency, business knowledge and awareness and technical proficiency. Additional technical training needed to ensure an audit can be effectively conducted should be arranged.
- Specific audit tools to improve efficiency and effectiveness of audits (such as for extraction and analysis of large quantities of data) should be identified and obtained where appropriate.
- In accordance with International Standards of Internal Auditing, the department should not undertake audit work where it does not feel it is sufficiently skilled to do so. In which case, specialised services or staff from either within the organisation or external to it should be considered and sought.

10. Advice and support

Internal Audit should not be required to:

- Perform operational duties.
- Operate controls, other than those within the department.
- Approve accounting transactions outside of the department.
- Implement controls that are the responsibility of management.

It is within normal accepted practice and International Internal Auditing Standards for Internal Audit to be requested to assist in a facilitative or consulting nature. Where this falls within the general remit of advising on risk and control this will be considered part of the service offering, with regard to resources available and time required.

Where it is agreed as appropriate for a member of the Internal Audit team to provide significant input to an activity or project that is beyond the normal remit, which means they should be temporarily seconded to another department or team, then the following measures will apply:

POL00401577

- The request will be approved jointly by the Head of Internal Audit and the Chair of the ARC.
- The resource impact on the approved audit plan should be approved by the ARC who will either approve the reduction in scope to the audit plan or request the Board to approve temporary resource to address the shortfall.
- The work conducted by the seconded member will be the responsibility of the receiving manager, not the Head of Internal Audit. The work will not be defined as internal audit work.

11. Standards of Audit Practice

The Head of Internal Audit will implement recognised International Internal Auditing standards and techniques such as those developed by the Institute of Internal Auditors, COBIT and COSO as appropriate to the Post Office.

Head of Internal Audit

_____ Dated:_____

Chief Executive Officer

_____ Dated:_____

Group Chief Finance Officer

_____ Dated:_____

Chair of Audit, Risk and Compliance Committee

_____ Dated:_____

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

3.3

Title:	Review against Terms of Reference 2019/20	**Meeting Date:**	19 May 2020
Author:	Rebecca Whibley, Assistant Company Secretary & David Parry, Senior Assistant Company Secretary	**Sponsor:**	Veronica Branton, Group Company Secretary

Input Sought: Decision & Noting

The Committee is asked to:

1. approve the outcome of the review against the Terms of Reference, confirming that the responsibilities under the Terms of Reference for financial year 2019/20 have been met, with the exception of the review and approval of the Internal Audit Charter and the approval of the Internal Audit Plan, both of which are due to be approved at the meeting on 19 May 2020; and
2. note the new Terms of Reference for the Committee adopted by the Board on 8 April 2020 to reflect the new Governance Framework.

Executive Summary

The Financial Reporting Council's (FRC) Guidance on Board Effectiveness 2018 refers to the need for "properly structured and appropriate terms of reference." As part of the annual Governance Report to the Board, the Board Committees review their Terms of Reference to see whether any changes are required and to evaluate whether the Committee's responsibilities have been discharged.

The complete review against Terms of Reference is available in the Reading Room alongside the old Terms of Reference applicable in financial year 2019/20.

As a result of the adoption of new Articles of Association for all Group Companies as requested by the Shareholder (Department of Business, Energy and Industrial Strategy (BEIS)) and the new Framework Document between Post Office Limited, BEIS and UK Government and Investments (UKGI), a new Governance Framework, including new Committee Terms of Reference, was developed. These new documents reflect the changes pursuant to the new Articles of Association and Framework Document and update the Terms of Reference to reflect practice that has developed over time as well as best practice in accordance with the FRC's UK Corporate Governance Code 2018. These new Terms of Reference for the Committee were adopted by the Board on 8 April 2020 and are effective from 9 April 2020. They are available in the Reading Room.

CONFIDENTIAL

POL00401577

3.4

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Audit, Risk and Compliance (ARC) Committee Evaluation 2019/20	**Meeting Date:**	19 May 2020
Author:	Veronica Branton, Company Secretary	**Sponsor:**	Carla Stent, ARC Chair

Input Sought: Noting, Discussion & Decision

The Committee is asked to:

- **NOTE** and **DISCUSS** the ARC Committee Evaluation for 2019/20 **(Appendix 1).**
- **APPROVE** the recommended actions to address points raised and areas which may require development.

Points raised/ areas for development:

All scores were above 3.5 (3 = "good/ at required standard") so there are no substantive issues to flag.

Pressure on agenda time was raised (as was the case last year, when the meeting times and numbers were extended) and one respondent noted a number of issues that it would be helpful to the Committee to cover: 1) a more strategic view of risks; 2) assessing management capabilities in the areas that report into the Committee; 3) IT strategy and the risks associated with this.

It was also suggested that additional IT expertise could be provided through the external auditors or the co-sourced internal auditors.

One of the lower scoring questions was how comfortable the Committee was that compliance with the regulatory landscape was adequately managed and reported. A paper on horizon scanning and a list of all the compliance activity and filings are being brought to ARC on 19th May 2020. The Committee is asked to consider whether this bridges any potential gaps in assurance or if any further reporting is required.

The Committee also scored "the management information received by the ARC and its timeliness (i.e. is it the right information at the right time to provide you with the assurance you need and the understanding of the business you need)?" a little lower than most questions. Committee Members are asked to flag any specific issues or measures they think would strengthen this reporting.

One respondent suggested that it would be helpful to move the May ARC meeting to June in future years because May was too early to review the Annual Report and Accounts (ARA) and July too late.

Recommendations:

i) Include the additional sessions proposed on the ARC agenda during 2020/21, in open or closed sessions, as appropriate

POL00401577

ii) Consider whether the pattern of meetings should change in 2021/22 to better fit the ARA timeline.

Previous Governance Oversight

The Nominations Committee approved the questionnaire at its meeting on 11th February 2020 and these reflected suggestions made by the Committee Chair. The Board noted the scores and comments from the Committee evaluations at its meeting on 8th April 2020.

Executive Summary

The UK Corporate Governance Code and the Corporate Governance Code for Central Government Departments[1] both stipulate that there should be an annual evaluation of the Board and its Committees which should be externally facilitated at least once every third year.

The Nominations Committee agreed at its meeting on 23rd September 2019 that the externally facilitated evaluation should be deferred until December 2020 and an internally facilitated evaluation run in March 2020. This was to reflect the changes in the Board and the wish for new directors to have attended a number of meetings before being asked to comment on their operation.

The ARC Committee questionnaire mirrored last year's to allow comparison across years but with a few additions; where the question is new this is indicated.

The Committee Members[1] and the Group Chief Executive, Group CFO, General Counsel, Director of Compliance, Head of Internal Audit and Head of External Audit were invited to complete the questionnaire[2] and all did. The questions, average scores and a summary of the findings are at Appendix 1.

Questions addressed

1. How have we implemented the actions from last year's Committee Evaluation?
2. What are the findings from the Committee Evaluation 2019/20?
3. How do last year's responses and this year's compare?

Report

1. Actions from the Committee Evaluation 2018/19

The actions from the Committee Evaluation 2018/19 were: 1) Increase the number of ARC meetings from 5 to 6 a year and focus the Committee's time on material risks. 2) Streamline reporting to the Committee to make papers shorter and easier to digest, focussing on material risks but with assurance provided on how the RCC is reviewing and testing less material risks. 3) Add in Non-Executive only discussions with Internal Audit twice annually. 4) Extend Internal Audit time on the ARC agenda when there is a red rated internal audit report. 5) Consider adding to the POL ARC agenda: presentations from business financial controllers / directors on their control and risk environments.

Seven ARC meetings were held during the 2019/20 financial year with the focus on material risks but with the minutes of RCC meetings provided for assurance that less material risks were being address at executive level. A combined Compliance, Risk and Internal Audit Report was introduced with separate papers provided where required. Non-

[1] Zarin Patel did not complete the questionnaire because she had only attended one meeting at the point the questionnaire was issued. Tim Franklin completed the questionnaire because he was a member of the Committee until the end of 2019.
[2] A "Not Applicable" option was included.

Strictly Confidential

POL00401577

Executive discussions have taken place with the internal audit team. External audit slots are included on the ARC agenda. Finance Directors and business unit heads have attended slots at ARC where appropriate, for example, Colin Stuart, Finance Director, reported on the reporting error in the Fin11 report for the Telco business caused by the inaccuracies in the Fujitsu data and Meredith Sharples reported to the Committee on PSD2 implementation.

2. Findings 2019/20

All sections within the questionnaire achieved an average score higher than 3.5 (3 = "good/at the required standard").

The higher scoring questions were:

3.	How would you assess the Chair's encouragement of debate within the Committee, including ensuring that all members are able to contribute to the discussion?	4.3
2.	How would you rate the Committee's understanding of the following areas of the Business: iv. Internal Audit	4.3
	i. Financial reporting and management	4.2
	v. External Audit	4.2

The lower scoring questions were:

7.	How would you rate the quality of papers and presentations received by the Committee?	3.6
8.	How comfortable are you that compliance with the regulatory landscape is adequately managed and reported?	3.6
9.	How would you rate the management information received by the ARC and its timeliness (i.e. is it the right information at the right time to provide you with the assurance you need and the understanding of the business you need)?	3.8
2.	How would you rate the Committee's understanding of the following areas of the Business: iii. Compliance	3.8

The scores and comments were positive, particularly about the chairing of the Committee, its composition, the value brought by the new external audit team and the work delivered by the internal audit team. The comments and recommendations were set against a high average score across answers and reflect the challenge of addressing the range and breadth of ARC topics across Post Office, addressing risk at a strategic level and being able to horizon scan as well as addressing the present day issues.

3. How do last year's responses and this year's compare?

There have been some changes in the membership of the Committee as Shirine Khoury-Haq stood down as a NED and Zarin Patel joined the Committee as well as changes in the executive and the external auditors, which has changed a number of the questionnaire participants. However, none of the scores have varied between years by more than 0.5.

POL00401577

4. Next Steps

If the Committee accepts the report's recommendations, it will be asked to consider the forward plan and the timing of committee meetings at its next scheduled meeting[3] on 27th July 2020.

[3] The additional meeting on 16th June 2020 is to review the ARA.

POL00401577

Appendix 1

ARC Evaluation Questionnaire 2019/20

	Question	2018/19 Average	2019/20 Average
A.	**Skills, experience, diversity, knowledge**		
1.	How appropriate is the composition of the Committee for the requirements of the business?	3.8	**4.1**
2.	How would you rate the Committee's understanding of the following areas of the Business:		
i.	Financial reporting and management	4.2	**4.2**
ii.	Risk	4.0	**4.1**
iii.	Compliance	4.1	**3.8**
iv.	Internal Audit	4.0	**4.3**
v.	External Audit	(new Q)	**4.2**
	Additional Comments: • We could benefit from additional independent IT expertise (which could be provided via the external auditors or the co sourced internal auditors). • In general I think the composition and skillset of ARC is excellent.		
B.	**Leadership, ways of working, time management**		
3.	How would you assess the Chair's encouragement of debate within the Committee, including ensuring that all members are able to contribute to the discussion?	4.2	**4.3**
4.	How effective is the Committee at focussing on the right issues?	4.0	**4.1**
5.	How effective is the Committee at providing both challenge and support to management?	4.1	**3.9**
	Additional Comments: My main concern about ARC is that the agenda is very full already. There are always additional things we could do but there are a few things that I think are gaps and where some time would be very worthwhile: - a more strategic view of risks, A good example is the good work that now seems to be going on in relation to the potential failure of a multiple partner. This arose in a somewhat obtuse way and should have been flagged by management if we were following a more structured process - assessing management capability, specifically in the areas covered by ARC - the finance function, risk, compliance and internal audit - IT strategy and risks where we have seen examples where risks have not been identified properly (e.g. Oracle termination of support) which has caused previous decisions to be reversed quickly. IT is also the bottleneck so often in the company's ability to implement change and improved service for Postmasters and customers.		
C.	**Information and Support**		
6.	How effective is the Committee at testing the information provided by its external advisers?	3.7	**4.1**
7.	How would you rate the quality of papers and presentations received by the Committee?	3.2	**3.6**

Strictly Confidential

POL00401577

	Question	2018/19 Average	2019/20 Average
8.	How comfortable are you that compliance with the regulatory landscape is adequately managed and reported?	3.6	**3.6**
9.	How would you rate the management information received by the ARC and its timeliness (i.e. is it the right information at the right time to provide you with the assurance you need and the understanding of the business you need)?	(new Q)	**3.8**
10.	How would you rate the access you have to any additional information and support you need to fulfil the requirements of your role (i.e. from management, secretariat or from external advisers, where required)?	4.00	**4.1**
11.	Are the frequency and length of ARC meetings appropriate?	Yes = 6 No = 2	Yes = 8 No = 2
12.	Are issues brought to the ARC at an appropriate time?	(new Q)	Yes = 8 No = 2
13.	Are there any issues or topics *that are not discussed* that should be considered at the Board?	(new Q)	Yes = 2 No = 7 Don't Know = 1
14.	Does the ARC have sufficient time in private to discuss matters of concern?	(new Q)	Yes = 5 No = 2 N/A = 2 Don't Know = 1
15.	**Please comment on the effectiveness of the interaction with Internal Audit.**		
	• Very effective – there is a very detailed, operational oversight and challenge given by Board/ ARC • Excellent. The Chair is always engaged and provides sufficient guidance and challenge. • In general Internal Audit is responsive and open. In general they do good work although their work doesn't always hit the mark (E.g. change spend processes). As with any IA function there is a balance to strike between rigour on the one hand and the need to maintain relationships with colleagues on the other. • IA continues to improve and deliver according to its Audit Schedule. • Effective and thorough - during the next year we may benefit from hearing from the co sourced Internal Auditors (Deloitte) more frequently • Open and sensible. • It's well-structured and timely.		
16.	**Please comment on the effectiveness of the interaction with External Audit. (new Q)**		
	• I don't have much visibility of this, but I have no concerns. • I think it is good. Regular dialogue with AC Chair. And discussions before and during the AC meetings. • Generally very good so far. • Sufficiently frequent. • Adequate • Effective both in and outside of the formal meetings. • Much better and very open. • It's well-structured and timely.		
17.	**Please include any thoughts you have about the operation of the Committee and any ideas for its future operation.**		

Strictly Confidential

POL00401577

	Question	2018/19 Average	2019/20 Average
	• Carla is an outstanding NED and Chair. She role models perfect behaviours and gives excellent honest challenge whilst understanding commercial realities as well as industry best practice in Risk and Compliance. • The Committee could support management more in the ARC remit particularly when the Board has made certain decisions which in turns has an impact on the management team particularly in terms of resource and volume of work. • This is one of the most effective Audit Committees I have seen. • I think the ARC operates well. It has to cover a lot of ground given the range of compliance and regulatory topics. It spends relatively less time on financial reporting matters compared to listed company audit committees – but that is understandable given POL has limited public reporting requirements and there are a wide variety of important areas to focus on. I think key members of the ARC are diligent in ensuring they properly understand topics and bring a lot of value, as well as being appropriately sceptical. • One point on timings – I would suggest that if possible going forward the May ARC is superseded by a June one so as to better mirror the timing of the annual accounts / audit. This year there is a separate June ARC call scheduled to focus on the accounts – which is helpful. May is too early. And July too late! • We can now rise up a level and use less time. • The compliance with the regulatory landscape is improving and the suggested steps to ensure that we have completeness, combined with the proposal for legal to input to the emerging compliance risks will be beneficial. • Carla Chairs the ARC extremely well given the breadth and complexity of the various businesses. • Well chaired. On occasions meetings can be rushed. Perhaps longer meetings should be scheduled in diaries with time given back if meetings under run.		

Strictly Confidential

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE REPORT

4

Title:	Criminal Misconduct and Cooperation with Law Enforcement Agencies	**Meeting Date:**	19 May 2020
Author:	Rodric Williams, Head of Legal (Dispute Resolution) Hannah Laming, Peters & Peters	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Decision & Noting

The Committee is asked to:

1. **APPROVE** the approach proposed in the "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 this approach, the ARC 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 Horizon HNGA is low or low/medium.
3. **APPROVE** the Tools supporting the Draft 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);
    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.
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.

Previous Governance Oversight

The Draft Policy was considered by the Risk & Compliance Committee on 6 May 2020. It 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.

POL00401577

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 will apply to all requests for support from law enforcement agencies. At present, it focuses specifically on seeking to address the risks connected to requests from Law Enforcement Agencies for Horizon data, given the findings in the Horizon Issues Judgment on its reliability and accuracy. The Draft Policy implements a risk-based approach to the provision of Horizon data. This approach is being built out for all categories of information request, in line with the paragraphs below:

1. The Draft Policy refers to requests from law enforcement authorities either for intelligence purposes or the provision of evidence (but not general data requests) from any party.
    a. Law Enforcement Agencies include the Police, intelligence agencies, public authorities such as DVLA, regulators and government departments. The Courts can also compel the provision of information and evidence.
2. It concerns matters where Post Office and/or its subsidiaries are asked to provide, voluntarily or by compulsory notice/court order, information it holds directly or through one or more of its 3rd party suppliers.
    a. All requests from Law Enforcement Agencies must be directed to Legal, Compliance or Security to manage.
    b. If requests are made that ask for information held by one of our 3rd party suppliers on behalf of Post Office (e.g., Fujitsu or Ingenico) the respective team will liaise with the contract owner (subject to confidentiality obligations) to help obtain this information.
    c. If the request is for information held by or on the systems/processes of a 3rd party supplier (and not on Post Office's behalf), we must direct the law enforcement agency to contact that 3rd party.
    d. If the request is about information held by or on the systems/processes of one of Post Office's business contracts (e.g., Bank of Ireland or Santander) we must direct the law enforcement agency to contact that 3rd party.
3. We can provide data to such Law Enforcement Agencies if it is for intelligence purposes only.
4. Where we know that there is an issue with the integrity of the data being asked for we must declare this to the requesting authority where that request is for intelligence purposes only.
    a. To date, we are aware only of issues in respect of Legacy Horizon and HNG-X following the Horizon Issues Judgement and must provide the "Advisory Notice" wording as set out in the Policy.
5. Where the data request is for evidence the request must be referred to Post Office Legal (or a nominated external lawyer), which will take a decision on what and how to provide the information to the law enforcement authority in accordance with the Draft Policy.

We are developing process flows for the different scenarios of information requests, which will be appended to the Draft Policy.

Strictly Confidential

POL00401577

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.

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 Horizon 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?

Strictly Confidential

POL00401577

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. The Draft Policy will apply to all requests for law enforcement assistance. It currently focuses on the specific issues arising from the provision of data deriving from Horizon following the "Horizon Issues Judgment" 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"). The key risks associated with the provision of Horizon data are 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

[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.

POL00401577

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.

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

8. The key risks the Draft Policy seeks to address with respect to Horizon data 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.

9. The Draft Policy will be built out to encompass any identified risks with other sources of data following further consultation with the business.

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

10. In the Horizon Issues Judgement, the judge 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.

Strictly Confidential

POL00401577

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.

POL00401577

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 on a voluntary basis with approval from the Board in higher risk situations;
    c. where evidence is provided on a voluntary basis without the approval of the Board in circumstances where the risk of adverse findings in relation to the integrity of HNG-A is low to medium-low; and
    d. where evidence is provided relating to data from historic Horizon systems on a voluntary basis but is accompanied by the appropriate advisory notice.

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

[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.

POL00401577

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.

26. Since January 2015, Post Office has only conducted three prosecutions on its own behalf. Those private prosecutions can be summarised as follows:
    a. GRO – a branch assistant who pleaded guilty on 5 November 2015 to three charges of theft from elderly customers by taking over their accounts;
    b. GRO – 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. GRO – a non-branch, GRO 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;

    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

POL00401577



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.

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).

POL00401577

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 made with reference to Tool 2: the *Provision of Evidence to Law Enforcement* tool.

36. In relation to data deriving from HNG-A: evidence relating to 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.

37. 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]

38. 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.

39. 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.

40. 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. Although there may not be a reason to believe that HNG-A data relied upon in such a case 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.

[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.

POL00401577

41. In relation to data deriving from HNG-X or Legacy Horizon, where evidence relating to any data other than Low Risk Data is sought, Post Office will provide an Advisory Notice before providing the data. This will flag to the law enforcement agency the risk that the data may not be reliable. If the law enforcement agency still seeks evidence relating to the data, it can be provided but the witness statement must contain wording equivalent to the Advisory Notice.

Monitoring of ongoing criminal cases (Draft Policy Tool 3)

42. 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.

43. 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)

44. 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.

45. 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

46. Where Post Office no longer conducts private prosecutions, it may consider that it is 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;

POL00401577

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.

47. 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.

48. 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 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.

49. 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?

50. 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

51. The Draft Policy currently focuses on the provision of data deriving from Horizon. Subject to ARC approval, we will incorporate law enforcement requests for other information into the Draft Policy and present it back to the ARC for approval.

POL00401577

Appendix 1

4

GROUP POLICY

Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct

DRAFT

Version – V0.2

Strictly Confidential

POL00401577

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

DRAFT

Strictly Confidential

POL00401577

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;
- 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;

[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.

Strictly Confidential

POL00401577

- 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 and other information to support to Law Enforcement Agencies and prosecutors for use in Criminal Investigations and prosecutions, including data derived from its Horizon computer system. 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;
- 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

POL00401577

- 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.

DRAFT

Strictly Confidential

POL00401577

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.

DRAFT

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

POL00401577

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

DRAFT

Strictly Confidential

POL00401577

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	

DRAFT

Strictly Confidential

POL00401577

DRAFT

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 will be provided where there is any reason to believe that Horizon data being provided as evidence may be inaccurate or unreliable in accordance with the "Provision of Evidence to Law Enforcement" Tool (Tool 2).	All Employees General Counsel General Counsel	
Law Enforcement Agency investigations	If Post Office becomes aware of issues with the reliability of data deriving from HNG-A and does not	Detective Control: Post Office Employees must notify Post Office Legal if they become aware of issues that may undermine the reliability or accuracy of	General Counsel	

POL00401577

and prosecutions	deal with these appropriately in the context 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.	data deriving from HNG-A (or subsequent versions of Horizon). 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	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.	Group Operation Director	

DRAFT

Strictly Confidential

POL00401577

	data by the defence. Post Office may therefore not have an opportunity to mitigate any risk this presents.	Preventative Control: 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).	Group Operation Director	
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	

DRAFT

POL00401577

		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	

DRAFT

POL00401577

	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	

DRAFT

POL00401577

		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	

DRAFT

POL00401577

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	

DRAFT

Strictly Confidential

POL00401577

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.

POL00401577

"**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.

"**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.

DRAFT

POL00401577

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 GRO 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: GRO

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.

DRAFT

POL00401577

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.

DRAFT

POL00401577

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

DRAFT

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.

POL00401577

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.



POL00401577

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.

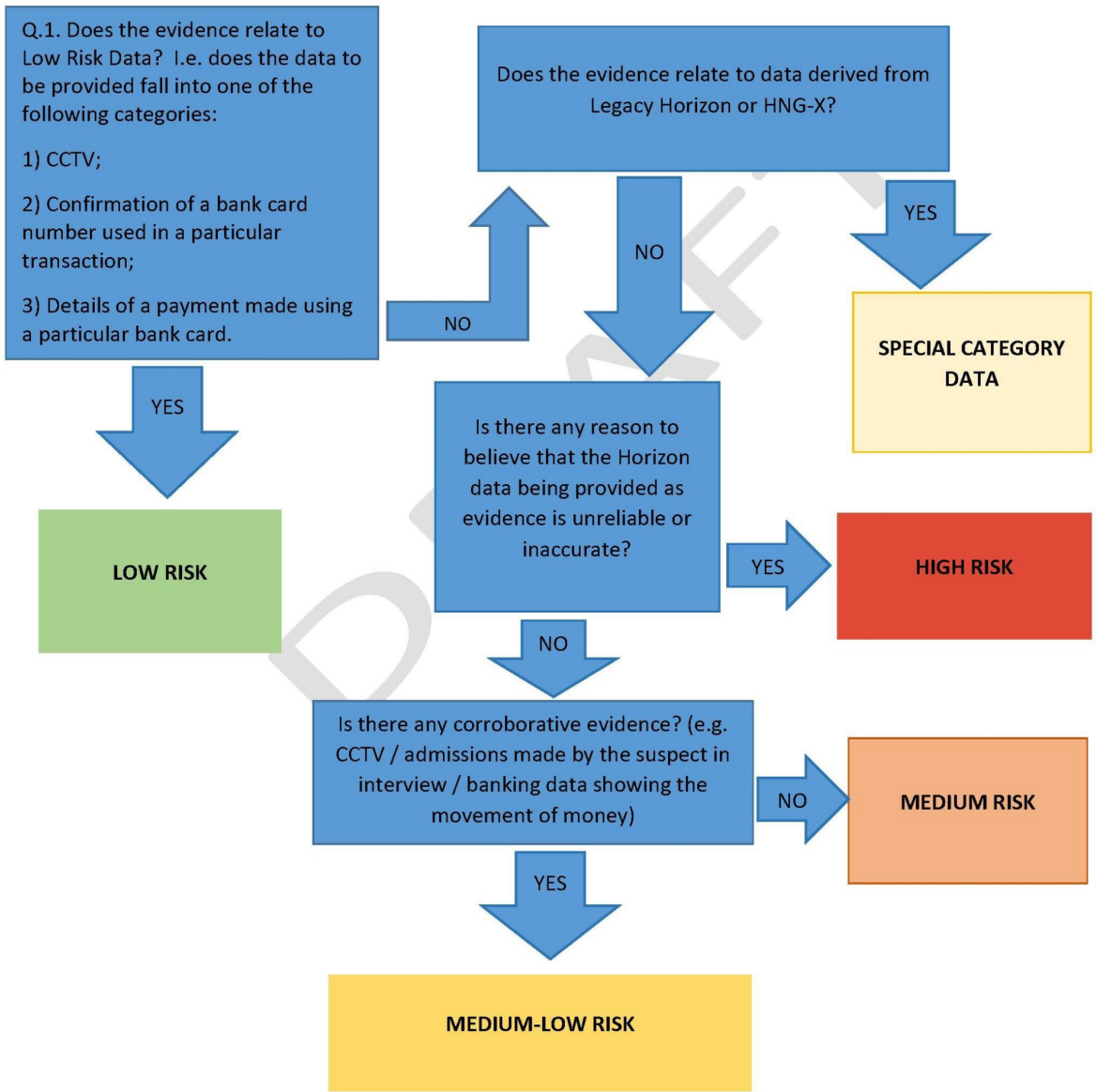
DRAFT

POL00401577

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:



POL00401577

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 a form of words which draws the recipient's attention to the potential reliability issue which has been identified. In addition, 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.
Special category data	Post Office **must** advise the Law Enforcement Agency of the risks associated with relying upon the data before providing it, by providing the Advisory Notice (as set out in Tool 1). If the evidence is still sought, it can be provided on a voluntary basis but the witness statement **must** include a form of wording that encompasses the content of the Advisory Notice (whether the evidence is provided voluntarily or subject to a Mandatory Order). The Disclosure Checklist (Tool 4) **must** be complied with.

Mandatory orders

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.

POL00401577

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.

DRAFT

POL00401577

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.

DRAFT

POL00401577

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.

DRAFT

POL00401577



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.

DRAFT

POL00401577

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);

DRAFT

POL00401577

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.

DRAFT

POL00401577

Appendix 2

4

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

POL00401577

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-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.

POL00401577

POST OFFICE LIMITED

Minutes of a meeting of the Audit, Risk & Compliance Committee (ARC), held on 24 March 2020, 09.00 - 12.00 hrs, 1.19 Wakefield, Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ/ Microsoft Teams Meeting[1]

5.1

Present:	**Invited Attendees:**
Carla Stent (Chair)	Amanda Bowe (Chair, Post Office Insurance ARC): Item 2
Ken McCall (SID)	Caroline Scott (Portfolio Director): Item 3
Zarin Patel (NED)	Tim Armit (Business Continuity Manager): Item 3
Tom Cooper (NED, UKGI)	Amanda Jones (Group Retail and Franchise Network Director, Interim): Items 4, 12
Regular Attendees:	Karl Oliver (Head of Commercial Partnerships): Item 4
	Sherrill Taggart (Legal Director, Interim): Items 6, 10
Tim Parker (Chairman, POL)	Mark Dixon (Head of Treasury, Tax & Insurance): Item 8
Alisdair Cameron (Group CFO)	Meredith Sharples (Director of Telecoms): Item 9.2
Andrew Paynter (Audit Partner, PwC)	Barbara Brannon (Procurement Director): Item 11
Stewart Light (Audit Director, PwC)	Andy Kingham (Head of Network): Item 12
Johann Appel (Head of Internal Audit)	Jeff Smyth (Group CIO, Interim): Items 13, 14
Mark Baldock (Head of Risk)	Tony Jowett (Chief Information Security Officer): Item 13
Jonathan Hill (Compliance Director)	Lisa Cherry (Group Chief People Officer): Item 16
Veronica Branton (Company Secretary)	Carol Murray (Deloitte, Director, Internal Audit)
	Lisa Harrington (NED, Observer)
Apologies:	
Ben Foat (Group General Counsel)	
Nick Read (Group CEO)	

1.	Welcome & Conflicts of Interest
	The Chair welcomed Lisa Harrington to the meeting as an observer. Lisa would be appointed as a Director of Post Office Limited on 8th April 2020.
2.	Update from Subsidiaries:
	Post Office Insurance ARC
	The Chair welcomed Amanda Bowe, the Chair of Post Office Insurance ARC, to the meeting. The written report was noted and AB provided an overview of the main discussion points at the Post Office Insurance ARC meeting, which had been held on 18th March 2020, followed by the PO Insurance Board meeting. The position in light of Covid-19 was changing rapidly and the team was working from home. The Covid-19 response had been discussed at the Board. It had been clear by 16th March 2020 that there was no market for travel insurance in the current climate and the sale of the product was suspended. This was a core product for the business. The ARC had taken the decision to proceed with the Nemesis programme for the home insurance business with the caveat that any material changes should be flagged to the ARC in the build up to "go-live" on 26th March 2020. The ARC had discussed the commission level PO Insurance paid PO Limited for audit services. This would need to be re-modelled in light of the market position and the lower volume of sales in branch. Al Cameron confirmed that he had asked the Post Office Insurance and central Finance Teams to review this. The ARC had also reviewed the PO Insurance dividend policy. In discussing the impact of the above and the implications for the validation of the goodwill on the Balance Sheet, Andrew Paynter noted that we were operating in unprecedented times and the impact on PO Insurance was particularly significant. PWC could not take a view on

[1] All participants joined remotely but the Company's registered office is 20 Finsbury Street.

POL00401577

POST OFFICE LIMITED

	impairment currently but would provide an update at the next Post Office Limited ARC meeting.
3.	Covid-19 (Coronavirus Implications for POL)
	The Chair welcomed Caroline Scott and Tim Armit to the meeting. The Covid-19 update paper had been circulated to the Board on 20th March 2020 and had been loaded to Diligent for information. **Structure and decision making processes** Caroline Scott provided an overview of the structure and decision making processes in place to respond to Covid-19 with the core objective to keep as much of the branch network open for as long as possible. The Group Executive had formed two Steering Committees to deal with the immediate response over the next few weeks and the longer term response over the next few months. A Rapid Response Team was operating which fed information from the functional subject matter experts into the immediate response Steering Committee. We wanted to be able to anticipate requirements rather that react to them but this was challenging as the position was moving rapidly. A number of points were raised, including: • what was the position on branch closures and had there been any comments from Government on cash and branch services? It was reported that Post Offices has been designated as essential services and could remain open. We had confirmed this to Postmasters at 7.30 am this morning. Exceptions to this were where Post Offices were situated in locations such as gyms. It was also noted that on any given day there would always be some branches shut. We were modelling around 1,000 – 2,000 shutting and at least 20% of the workforce self-isolating or ill. 1,800 FTE of our workforce is over 70 and therefore classified as high risk. IRRELEVANT IRRELEVANT Deposits were down slightly after a spike at the weekend mainly driven by small business deposits. Cash withdrawals had increased steadily. We were plotting out the impacts on our security headroom. Supply chain was operating and we were having conversation with G4S and Loomis about back up arrangements. • Tom Cooper noted Post Office's request to Government for a security headroom relaxation and for a waiver for maintaining 11,500 branches in the current climate. Consideration was being given to modifying the covenant rather than giving access to the full funding amount. There was support for waiving the branch number requirements but UKGI/ BEIS were discussing how long that should be for. Post Office would be asked to produce a plan for building branch numbers back up when we were closer to moving back to normal working conditions. Consideration was being given to revenue shortfall and the extra costs associated with branches closing (as distinct from extra change spend). • We were looking at solutions to address loss of service in areas where Post Offices closed. We were seeing significant increases in branch closure numbers but not yet at the maximum level used for modelling. • Tom Cooper noted that the Government community hub announcement had been made and that BEIS should have co-ordinated with Post Office about this • The timelines for the spending review had not yet been changed and if the review proceeded Post Office would need to submit a bid. We would need to work through the figures for the coming year based on a number of scenarios such as branch numbers declining by 20%. The Post Office Finance Team had met with UKGI/ BEIS and would be meeting with them again later today. A financial viability review would be produced for the Board meeting on 8th April 2020 with low, medium and high scenarios. There would be

5.1

POL00401577

POST OFFICE LIMITED

	some scenarios under which Post Office Limited would no longer be able to trade unless the current rule set was changed. Product sales were volatile in the current climate and whilst we hoped the position might have stabilised by the end April there was no certainty of this. We would aim to have a budget position for 2020/21 by the end of April 2020, including whether we were likely to break even. **Business continuity plan** Tim Armit described the contingency planning in train to maintain Post Office services; this included spatial gapping, monitoring the payments and cash flowing into branches, anticipating the need for additional staffing support in the network and working through how this could be provided, noting, for example, that 1,800 of our Postmasters were over 70. Our call centres were operating remotely and we were planning to provide more pop up Post Offices through Post Office in a Box. It was also reported that Russell Hancock, Supply Chain Director, was investigating a number of options for using agency staff and was working with Loomis to get cash into branch. We were focused on keeping our ATMs loaded to serve our vulnerable customers under POca. We were also exploring home delivery options. A number of points were raised, including: • who was looking at regulatory gaps that could emerge during this period of operation and how were we considering heightened areas of risk such as cyber security? The heightened risks in areas such as cyber security were acknowledged and Tony Jowett, CISO, could address our response during his agenda item. Mark Baldock was engaged with the Rapid Response Team's work and was in contact with areas of the business such as the CVIT team where risks were now greater. The risks we faced in the current circumstances and the timescales in which they might emerge were being documented, as were the regulatory impacts • there needed to be clarity on what the priorities are. It was reported that we were in direct contact with our regulators and partners to ensure clarity of understanding on these points • would there be any increased monitoring during this period, for example on mystery shopping? It was reported that mystery shopping would be suspended during this period but that the number of financial services transactions had also reduced. We were focussed on making sure that the core services could be deployed across the network and some people might need to be re-deployed to other roles. Additional spot checking and sampling were discussed and under consideration by the Compliance team and the volume of complaints and cancellations was also being monitored. • It was noted that the position was changing rapidly. PWC was seeing many clients under extreme stress and the FCA had told listed companies not to post their preliminary financial announcements. The Chair thanked all the teams for the work they were doing in pressurised circumstances. It was noted that it would be helpful to keep the Board informed in the most streamlined way possible.
4.	<u>Partner Failure Contingency Update</u>
	The Chair welcomed Amanda Jones and Karl Oliver to the meeting. Amanda Jones provided an overview of the partner failure response plan. McColls' financial position had been of concern but they were trading well in current circumstances because many branches were in neighbourhood convenience locations; they were rationalising their estate and had reduced their Post Office franchise by 31. McColls had been open with Post Office about their financial position, trading position and loan arrangements and their financing had been extended. Our broader contingency planning for Covid-19 included modelling service provision for our priority group. Service provision for POca customers and proximity to other branches were

POL00401577

POST OFFICE LIMITED

	partners to fail or decide not to operate Post Offices were key criteria; we then looked at where we needed to put plans in place. Re-deploying temporary operators, our own people and/ or using outreach options were part of this contingency. We were also talking with the big six supermarkets about putting a Post Office in a Box into their locations should we need to and this idea had been received positively. A number of points were raised, including: • had we broadened the net to consider which other partners might be vulnerable e.g. IRRELEVANT It was reported that IRRELEVANT would be able to operate as they were IRRELEVANT nd were planning to continue trading where they operated a Post Office; however, their travel business had been very badly affected and we were in contact with them daily. The ARC **NOTED** the partner failure response plan.
5.	Minutes and Matters Arising
5.1	The ARC **APPROVED** the minutes of the meeting held on 28 January 2020.
5.2	The ARC **NOTED** the progress with completion of actions as shown on the action log most of which were covered through papers included on today's agenda. Andrew Paynter and Rosie Clifton were asked to provide examples of best practice for contract management (5.3 28/01/2020) It was noted that it might be necessary to review change prioritisation and where we needed to pause or slow down projects to have the capacity to address the immediate response to Covid-19. An update on Successfactors was included under any other business but a fuller review would come back to the July 2020 ARC meeting.
5.3	The ARC **NOTED** the draft Risk and Compliance Committee minutes from the meeting held on 9 March 2020.
6.	Annual Legal Risk Report 2019/2020
	The Chair welcomed Sherrill Taggart to the meeting. Sherrill Taggart provided an overview of the legal risks and it was noted that competition risk should be green rather than amber. A number of points were raised including: • many of the risk mitigants were reliant on training, was that going to be possible in the current environment? It was noted that internal training would need to be prioritised and some training may need to be deferred. In addition, we had been reviewing the costs associated with using external trainers. We were working with the legal panels to find creative solutions to training requirements. ARC members agreed that people's attention was not likely to be on training at the moment but we needed to maintain focus where there were risks. The Committee requested that deferrals of training of high risk areas be brought to their attention. • the contract management framework would be discussed later in the agenda but it was noted that we would be focussing on the top contracts and the key areas of risk in the current environment. The Committee requested that any issues relating to the Top 15 contract be brought to their attention at each meeting. • the current environment required us to consider how robust our partners and suppliers were as well as our own trading position. It was noted that we were putting in place a due diligence approach with our key partners, including where we might need to trigger a force majeure clause; this would be circulated to the ARC when finalised. **Action: Sherrill Taggart** The ARC **NOTED** the report and endorsed the current actions designed to mitigate the risks illustrated as well as the further actions requested at the meeting.

5.1

POL00401577

POST OFFICE LIMITED

	Sherrill Taggart would bring a revised plan to the next ARC meeting setting out how we were going to bridge any gaps in contract management. The focus on the top 15-30 contracts would help us understand where we had any issues with those contracts or the management of those relationships. **Action: Sherrill Taggart**
7.	2020/21 Internal Audit Plan
	The Chair welcomed Carol Murray, our insourced audit partner, to the meeting. Johann Appel introduced the 2020/21 Internal Audit Plan and explained the approach now proposed to address the response to Covid-19, including bringing forward the review on cyber risk. The Internal Audit Team would be finalising in-train reviews and should still achieve a meaningful outcome. The Internal Audit Plan would be re-prioritised to focus on greatest risk and those audits suitable for remote review. This might include splitting some planned audits, such as Joiners, Movers and Leavers (JML) and Cyber Security, into parts to focus on the main risks. The Internal Audit Team would need to focus on how it best supported the business at this time. Looking across their client base, Carol Murray noted that businesses were in a state of flux but a number of steps were being taken by clients: • review and re-order audit plans, aligning this with the risk management function • offer Internal Audit support to the rest of the organisation where value could be added • some retail clients were asking their Internal Audit teams to review and test their business' approach to responding to Covid-19. It was also noted that Post Office Limited's Internal Audit contract allowed it to deploy the Deloitte resource as appropriate. A number of points were raised, including: • was Internal Audit involved in planning the response to Covid-19? It was reported that Internal Audit had been involved informally and had also been involved in providing advice to Post Office Insurance. The ARC felt that it would be useful for Internal Audit to have an overview of the Covid-19 response to help identify where the key risks might lie • a number of planned audits, such as Postmaster remuneration which linked into the post GLO work, should proceed but others, like digital strategy, may not be needed to at this juncture • that we needed a revised plan that reflected the current environment and the top five priorities. We also needed a monthly update from Deloitte on the external environment, including risks and the approach other companies were taking to managing their risks and running their businesses **Action: Johann Appel/ Deloitte** • that the Postmaster Remuneration review would need to look at whether lessons from GLO had been learnt • we had to make sure that the scope of Internal Audits was right. In the case of Postmasters, the focus had been on methods and processes for providing communication but we also needed to know if the information itself was fit for purpose. Johann Appel noted that the team was also undertaking a review of agent on-boarding • we would need to test our basic processes such as handling cash and stock controls (including Stamps), especially if there was going to be a spike in temporary staff. Johann Appel would circulate a revised plan in advance of the next ARC meeting. **Action: Johann Appel**
8.	Treasury Policy
	The Chair welcomed Mark Dixon to the meeting. Mark Dixon provided an overview of the changes to the policy which were not substantial as an in-depth review had been undertaken in March 2018. The changes proposed were to:

5.1

POL00401577

POST OFFICE LIMITED

	• ensure consistency with the Group Governance Framework and revised Articles of Association • delegate authorities to the Group Chief Finance Officer, the Director of Tax, Treasury & Supply Chain Finance (TTSCF) and the Treasurer, which were the roles and titles existing as at March 2020. The document had also been updated to ensure that where titles changed over time authorities would rest with those persons performing substantially the same roles • update Sections 5 and 6 to reflect changes to credit ratings over the last 12 months • update Section 11 so that: all new bank accounts required the approval of the Group CFO; additions to a mandate or Authorisation Panel, or the granting of administrator access rights to an Internet Banking System, required approval by the Group CFO; and removal from a mandate or Authorisation Panel, or the removal of administrator access rights to an Internet Banking System, would be approved by any one of the Group CFO, the Director TTSCF or the Treasurer. Assurance was sought that Post Office Limited's controls around payments were sufficient for a home working environment and what contingency arrangements were in place. It was reported that the levels of controls were the same as being in the office but that certain functions, such as writing cheques, could not be undertaken. The ARC **APPROVED** the Treasury Risk Management Framework, Policies and Authorities as set out in the paper and appendices presented.
9.	Consolidated Report from Risk, Compliance and Internal Audit
9.1	Risk Report
	Mark Baldock provided an update on the risk management work that had been taking place, including a session on risk enterprise with the Group Executive in February 2020. 14 risk enterprise categories had been identified with 50 business risks feeding into this. This information had been loaded onto Archer and would be brought back to the next ARC meeting. In response to questions, MB conformed that the previous set of risks had been incorporated into the new schedule. The risk appetite statements were being developed but the timings for this work would be reviewed in light of the current priorities. The Covid–19 response would be the main focus for the Risk Team in the next period. The Covid-19 specific risks would be added onto Archer. A number of points were raised, including: • were there any risk items of concern or anything not captured because of Covid-19? It was reported that supply chain and our partners were a particular focus currently. We were working through how we would operate with, say, a 20% decrease in staff numbers and agents. Back-up arrangements for the POca and Telecoms call centres were high on our agenda but that Telecoms had managed to arrange for home working for 50-100 staff wheras some other companies had needed to stop call centre services where home working security could not be guaranteed. The ARC **NOTED** the status of the current enterprise risks; the status of the key business risks (including Coronavirus); the latest position on the review of the Post Office's enterprise risk management (ERM) function (including a refresh of its enterprise risks); the latest position on the implementation of the Post Office's Governance, Risk & Compliance tool (Archer); and the status of the Change Portfolio and key delivery challenges.
9.2	Compliance Report
	The Chair welcomed Meredith Sharples to the meeting to discuss Telecoms compliance issues and the resilience of operations in the current environment. Meredith Sharples reported that our Telecoms calls centres were based in Preston and Selkirk. There were around 350 staff and absence rates were running at around 30% with a 20% increase in demand. Home working was in place for 50 members of staff and this is growing. Post Office was focussed on

POL00401577

POST OFFICE LIMITED

	ensuring service delivery to our elderly and vulnerable customers. We expected further increases in absence rates and were working with TalkTalk and BT Openreach to monitor provision of service. We were seeing significant demand on our networks and chargeable call volumes were currently up by 25%. We had written to Ofcom to ask for suspension of End of Contract Notification letters to enable us to focus on core delivery and cognisant of the strain on the Fujitsu call centre. Ofcom had advised that it would respond to us by end of week. We were looking at how we could reduce unnecessary calls to the contact centre. It was reported that the interim solution to address PSD2 non-compliance would be in place by the end of April 2020, whereby credit for the calls which customers should not have been charged would be paid back monthly in arrears. The fully compliant solution was harder to implement as technical build changes would be required to avoid charging customers for these calls in the first place. Initial views were that the Fujitsu cost for this work could be around IRRELEVANT and could take up to a year to build and deploy. It was agreed that the business would continue, for the small number of customers impacted, to correct the charges monthly in arrears. A number of points were raised, including: • was any action required on POca and on managing our relationship with Fujitsu? It was reported that we had been considering back up for call centres but this was challenging because Fujitsu did not have built in resilience Jonathan Hill provided an overview of the main compliance issues: • we had provided the information required to Ofcom in relation to Freephone call numbers and data on engineer visits and were preparing a reserving rights letter to send to Fujitsu • the Information Commissioner's Office (ICO) was comfortable with the approach we had taken to the e-mail data breach • we were working through our approach to implementing the requirements for Cookies but were checking whether the situation with Covid-19 would affect our ability to deploy the solution by the end of April 2020 • GDPR remediation – there were only 38 contracts left in negotiation but this might be one of the projects that needed to be paused subject to ARC's agreement. It was noted that that decision could not be taken today and ARC would need to consider re-prioritisation requirements • the Ofcom investigation into Text Relay has been formally closed as we have paid the £175k fine • the Compliance Team was working with regulators, our regulatory principals and the business to ensure that compliance processes were appropriate and do not create an unnecessary burden on the front line, whilst maintaining our compliance integrity ARC Members requested that the Compliance team consider what other controls might need to put in place during this period. The ARC **NOTED** the report and **APPROVED** the Regulatory Breach Protocol.
9.3	Internal Audit Report
	Johann Appel reported that seven Internal Audit reports had been finalised since the last ARC meeting. Fieldwork had been completed face-to-face in most instances for the other work in train and these reports were being drafted. The vetting and Fit and Proper review would come to next ARC meeting. The effectiveness of the compliance function was the only report on the plan that had not been started and consideration would be given to whether this should be postponed given the focus on responding to Covid-19. There had been a report from Meredith Sharples at the last ARC meeting following the Telecoms Internal Audit report. It was noted that th IRRELEVANT ebtors' balance issue had been picked up by the central Finance Team in Q1 but the Fujitsu reports did not contain sufficient detail to be able to take action; resulting in an overstatement of debtors. Al Cameron noted that we should have been faster in addressing the issue and that Grant Thornton had been

POL00401577

POST OFFICE LIMITED

	engaged to assess the quality of Fujitsu reporting given this and previous instances of shortcomings in their reports. Remedial management actions were in place but while Fujitsu remained a partner we could continue to have problems with the quality of reporting which meant our oversight needed to be greater. AC noted that Finance had been in the middle of team restructuring when the Covid-19 crisis had struck. The GE minus 1 structure was in place for Finance but we might not be able to go beyond that currently. The Finance leadership team were planning to undertake a capability review at the same time as determining the new structure, looking at how we could benefit from automation and use human resource predominantly for analysis. Mark Baldock noted that the risk of non-compliance had been identified for the Telecoms business but had not been given the right visibility. The Risk Team would be running a workshop with the Telecoms business regarding ownership of risks identified and flagged by another function, such as Risk or Compliance. The ARC **NOTED** the progress being made with delivery of the Internal Audit programme and completion of audit actions.
10.	<u>Contract Management Framework Update</u>
	Sherrill Taggart reported that 143 material contracts had been identified together with their contract managers. The pilot on contract management had been split into two phases: obligation mapping for contract management which would be completed by 21 March 2020 and a second phase which was due for completion by 26 May 2020. Staff resources were in place, 20 contracts had been uploaded the Source to Settle (S2S) system currently and internal contract manager training provided for these contract owners. External training was not proposed currently because of the cost and in light of the current focus on the Covid-19 response. ST noted that the contract management role and business as usual requirements may be difficult to manage in some instances where an individual is both responsible and accountable for the execution of the contract and its management. A number of comments were raised, including: • that the failure to locate 78 final, signed contracts seemed like a basic process failure. This was acknowledged and it was noted that we had made progress in tracking down some of these contracts, most of which were older contracts, and that we had the 30 most material contracts in hard copy. The issue would be resolved for the future through using the S2S system. We were continuing to look for missing contracts but it was difficult to identify owners for older contracts and where we could not we might need to ask the supplier for the contract • ARC members were concerned about compliance in this area but also workload issues for key individuals. Al Cameron agreed that this was an important piece of work involving cultural change, compliance with process and, in addition, organisation design work would need to factor in contract management requirements so that responsibilities and accountabilities could be allocated appropriately and with clear accountability. Nineteen individuals were responsible for managing 46 of most material contracts alongside their core roles and this was not a viable model. The ARC: • **NOTED** the progress made to date in piloting the implementation of the Contract Management Framework (CMF) and the delivery date for the Pilot moving by 9 weeks from 24 March 2020 to 26 May 2020, noting that the deadline could change again because of re-prioritisation in response to Covid-19 • **AGREED** that a paper should be brought back to the next ARC meeting with a dashboard for the material contracts, the contract owner, which contracts were missing, which had been loaded to S2S and which contracts were due for renewal in next 18 months or so. **Action: Sherrill Taggart**

POL00401577

POST OFFICE LIMITED

11.	Managing Procurement Relationships
	The Chair welcomed Barbara Brannon to the meeting. Al Cameron explained that Barbara had joined Post Office with the brief of improving controls and transparency in procurement and significant progress had been made. Using the Crown commercial services framework or carrying out a fully compliant OJEU tender process were the only way of ensuring full compliance because other routes were difficult to evidence even where our view was that no other provider would able to provide the service. We managed any material risks associated with non-compliance carefully. There had been instances, for example the contract with Fujitsu, which the Board had approved even though it was non-compliant, but we knew that no-one else would be able and/or would want to provide the service. Barbara Brannon provided an overview of some of the procurement issues we faced and instances where we had accepted a process that was not fully compliant and the reasons for this. We were actively putting in place Post Office frameworks to be able to call off services and ensure that we were more compliant. A number of points were raised, including: • were we taking procurement concerns seriously enough? Concern was expressed about taking risks with Public Contract Regulations (PCR), especially in the current environment, where a reason of "business preference" was unlikely to stand up to external scrutiny. The ARC requested a Board level policy on procurement compliance setting out when we might consider accepting non-compliance, noting that there were instances where we would need to accept this risk. The procurement thresholds should be considered as part of the policy • that we needed to consider what behavioural changes were required and make sure that non-compliance and poor contract management had consequences. It was critical to drive compliance with the law and the Board needed to oversee this, particularly in light of a recent instance with the global payments contract extension • AC noted that Barbara Brannon had done an excellent job of improving the procurement processes, creating transparency in the procurement pipeline and that instances of non-compliance had been sanctioned by the GE; a paper would be brought to the Board and a regular update provided to ARC which included the General Counsel's view of legal risks It was AGREED that Al Cameron would convey the ARC's views to the GE and that a paper would be provided for Board on 8th April 2020. **Action: Al Cameron** The ARC **NOTED** the report which set out breaches to Post Office governance, key controls around contracts and the extent of compliance to PCR regulation in the award of contracts.
12.	Selling Regulated Products in the Branch Network
	The Chair welcomed Amanda Jones and Andy Kingham to the meeting. The ARC **NOTED** the paper which addressed questions around the ability of the branch network to compliantly introduce and sell regulated products. Regulated products included Post Office Insurance (POI), Bank of Ireland (BoI), Telco and Royal Mail products. These products in isolation were not complicated to sell, however with c. 120 different transaction types in the majority of branches, this made keeping colleague product knowledge and operational understanding up to date challenging. For Financial Services, improvements had been planned to ensure that the selling practices for insurance products improved. For Mails, specifically in relation to Dangerous Goods conformance, further intervention was needed to achieve the required performance standards. Amanda Jones noted that consequence management for non-compliance was needed and we were considering which branches might be required to stop selling regulated products. A number of points were raised, including:

Strictly Confidential

POL00401577

POST OFFICE LIMITED

	• that a 42% compliance rate could not be tolerated and the paper did not set out a comprehensive action plan. A robust plan needed to be put in place and this should include owners and due dates. It was noted that in 9 out of 10 instances Postmasters and agents were asking the safety questions about a parcel's content but were failing in their compliance with other questions that they should be asking. We were trialling a different approach and looking at how more onus could be placed on the customer to attest to the content of their parcel • the cost and challenge of installing pin pads was noted in the paper but a technical solution was needed to underpin the other measures discussed • it would be helpful to see the footprint of non-compliant branches to understand if there were any discernible trends • there appeared to be a disconnect between customer complaint figures and the mystery shopping results. It was noted that adherence to processes by Postmasters and agents was the key issue here and that the reviewing the level of complaints should not be the primary measure of compliance . We were not comfortable with this situation but were within tolerance on customer complaints. It was noted that we had been asked to suspend mystery shopping in the current environment but the Compliance Director would be discussing other ways of issues being picked up in the network with the ARC Chair. It was **AGREED** that an action plan would be created and provided as part of the next Compliance Report to the ARC. **Action: Amanda Jones/ Karl Oliver**
13.	PCI-DSS and Cyber Security Update
13.1	PCI-DSS
	The Chair welcomed Jeff Smyth and Tony Jowett to the meeting. Jeff Smyth introduced the report. Ingenico had advised that they wanted to undertake a legal review of all in-flight contracts. The company had stepped up their WFH arrangements and all the technical requirements had been set in train. We had asked about the implications of WFH on testing requirements and received adequate assurances. We were carrying out field trials on supplying a post office on wheels. We had an approach in place for an over the telephone arrangement for Verizon and had a backup option in place. A number of points were raised, including: • could we say whether we would be able to remain on track with the timelines for obtaining PCI compliance? It was reported that there were no indications at this stage to suggest that there was not the people or technical support to deliver to time. Cross organisational integration testing was potentially difficult to deliver but that was not due to take place in the next couple of months. We had waivers in place for the delivery of certain services such as global payments • that the ARC had requested regular confirmation in writing from the Fujitsu and Ingenico CEOs that work was on track from their side. Jeff Smyth would respond to the ARC on what we could put in place and the time period for reporting adherence to timelines **Action: Jeff Smyth** • were we rolling out our PCI software mid-year rather than in Q1? It was reported that our timetable had not changed but we would only come out of moratorium after Christmas. There would be an automated roll-out of software with electronic rather than physical deployment. The ARC **NOTED** programme progress in the last reporting period.
13.2	Cyber Security Update – includes update on Joiners, Movers, Leavers
	Tony Jowett introduced the report and in response to a question on what additional activity was taking place to address heightened risks in the current climate, noted that we were talking to our third party advisors about dark web risks and how we could protect against these. There had been instances cited externally of spam emails being sent which contained

POL00401577

POST OFFICE LIMITED

	ransomware. There were also challenges associated with protecting our data while employees were WFH. Guidance had been issued on protecting Post Office data, including accepting valid patches and upgrades straight away and not downloading data where not necessary. TJ noted that we were in the final stage of data collection for the Cyber Security resilience work and would be scheduling the Deloitte review of our maturity level in May 2020, subject to assessing whether this work could be done effectively with remote working. Good progress had been made in the Joiners, Movers and Leavers project but more work was needed on our third party providers such as audit and log data. We were working with Deloitte on what Post Office would do if attacked by ransomware. TJ also had regular meetings with the FRES CIO. Last year, an external "Red Team" test had taken place to test how difficult it was to breach the Post Office systems but a recent "Red Team" exercise had focussed on how Post Office could be compromised from the inside and what could be done from a Post Office laptop currently that should be disabled. Post Office IT would be circulating guidance on Covid-19, especially in relation to social media and privacy settings. Concern was raised about the ease of the insider attack and it was noted that this was in context of the majority of our work having been focussed on external threats. We needed to go back and look at some of the activities Computacenter ran for us and undertake audits of this. The ARC **NOTED** the status and plans to achieve agreed target maturity levels; the status and plans to achieve a reduction of risk associated with Joiners, Movers and Leavers; the status and plans regarding our response to recent ransomware events; the status and mitigation plans regarding the recent "red team" test.
14.	<u>Review of IT Controls</u>
	Jeff Smyth introduced the report. We had a commitment to using COBID as a control self-assessment framework. We are assessing the resilience of our external suppliers as they were single points of failure (particularly Fujitsu and Computacenter). We are considering retention and knowledge loss associated with failure to retain key staff. We are assessing other controls and compliance reporting arising from running the IT. JS is working with Internal Audit to conduct a desktop based walk through of all self assessments which would take until May 2020 to complete. The review is of both "run IT" and "change IT" controls. Focus is on 3 key areas: AML of suppliers, insider and cyber threats and knowledge retention and loss. JS is seeking to move from a basis of self attestation to more robust testing and reporting. A number of points were raised, including: • could we focus on the controls not operating as required as we did not want to be risk accepting for an extended period of time? It was reported that we had identified the key risks that we should be focussing on • it was noted that the report stated that IT controls had last been reported to the ARC in 2018, however, the Internal Audit report on IT controls had been discussed by the ARC in May 2019. We needed to ensure regular reporting to ARC. The ARC **NOTED** the status of IT Control Framework and the progress made.
15.	<u>Audit Update</u>
	Andrew Paynter provided an overview of the proposed audit process, noting that significant thought would be given to how the audit would be run remotely. PWC thought they were

POL00401577

POST OFFICE LIMITED

	fairly well placed to conduct the audit remotely and had discussed this with Tom Cooper and Al Cameron. There were likely to be some limitations on how PWC carried out its corporate reporting. The GLO audit risks needed to be increased again having initially settled with the claimants and now offering historic claims settlement process. Going concern could not be signed off without funding being in place. We would need to determine whether an impairment was needed for the goodwill valuation for Post Office Insurance. AP also noted that PWC relied on the Horizon and Credence controls systems when carrying out the audit. Stuart Light explained the scope of the audit of the Credence and Horizon systems. Seven deficiencies had been identified, two of which were categorised as high and one as medium; related to management access to these systems. Checks on the activities undertaken where there had been unauthorised access to the systems had been carried out and in these instances no material activities had taken place. The finding categorised as high for the Horizon system related to 10 employees who were not removed from system in a timely manner after they had left Post Office Limited. All were DMB employees and their accounts had not been used inappropriately after the leaver date. This shortcoming should be addressed as part of JML Project so should be resolved by next year. The finding in relation to global users related to individuals with high end privileges to the Horizon system. A bi-annual review had been put in place subsequent to year end (in January 2020) but because this had not in place for the whole of the year under review it remained as a finding. All activities undertaken by these users had been appropriate. The finding categorised as medium was a single incident in relation to a user of the Credence system who had not received the appropriate approval before joining system but had only been granted reader access. This shortcoming should also be addressed through the JML Project. Andrew Paynter noted that Post Office Limited needed to ensure clarity of responsibility for processes. ARC members re iterated that the JML Project must be concluded. Al Cameron reported that Traction software for monitoring internal controls supported by PWC was used widely in the organisation and that, due to limitations on services that can be provided by external auditors, we needed to move off this system. The plan was to move everything onto Archer after testing migration issues. Mark Baldock would report on the progress of this work in the next Risk report. **Action: Mark Baldock** The ARC **NOTED** the update.
16.	<u>Any other Business</u>
16.1	Update on Success Factors
	The Chair welcomed Lisa Cherry to the meeting. Lisa Cherry explained that a deep dive on Successfactors was going to be brought back to ARC meeting in July 2020. Deloitte had been brought in to provide external support and were three weeks through a four week review. We proposed staying on the Successfactors system which was ranked as one of the best systems available and in which we had made a significant investment; however, we were not getting the best from system currently. The configuration had been at a basic level which did not align with the HR operating model and therefore required workarounds. There were a lot of rule based permissions which added complexity. There were instances where our interpretation of GDPR had been incorrect, overly restricting access to the system and leading to single points of failure. We were prioritising resolving these issues to enable best use of the system.

POL00401577

POST OFFICE LIMITED

	The Chair thanked Lisa Cherry for progressing this work and was encouraged by the progress made.
16.2	Stamps Reconciliation
	Al Cameron introduced the paper. Last summer we had become more concerned about how we managed stamps because there were a significant number of branches where we did not receive a reconciliation for stamps. Postmasters were responsible for reconciliations on Horizon but Post Office used the Galaxy system for reconciliations and we needed to put in the right reconciliation controls between Horizon and Galaxy. Our hypothesis was that the reconciliation gaps created ups and downs in accounts but did not lead to Postmaster losses, however we want to test that this is the case which was why we wanted to commission an external audit. The audit findings would be reported back to the ARC and the Board. A number of points were raised, including: • Why would Ben Foat be the owner of the audit as these were operational and accounting issues? It was reported that there were two distinct pieces of work. The Steering Committee led by Tim Perkins and sponsored by Al Cameron would drive through the practical changes we needed as a project. The audit to test our hypothesis that Postmasters would not have not been out of pocket historically would be sponsored by Ben using third party resource. • the fact that this issue had not been discussed previously at the Postmaster Litigation Subcommittee was raised. It was agreed that this should be discussed at the sub Committee but the work to gather the evidence and assess the facts, including whether the reconciliation position evened out over time or if we could be open to criticism for asking Postmasters to make good balances, should proceed. In response to this point, it was noted that Postmasters were responsible for booking stamps in so timeously. • how sure were we that this problem didn't exist more than five years ago? It was reported that we would be asking this question but we believed that the controls had been stronger in previous years. The ARC: 1. **NOTED** the background and legal position set out in the paper 2. **APPROVED for recommendation to the Board** to appoint an external accounting firm to investigate the issues in this paper but noted that we should not use any firm which had provided advice on the GLO 3. **APPROVED for recommendation to the Board** that a 'working group' and 'SteerCo' be formed to manage and oversee this work stream and that it should produce recommendations.

5.1

Strictly Confidential

POL00401577

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 12 May 2020

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
24 March 2020					
5. Minutes and Matters Arising					
5.2	An update on Successfactors was included under any other business but a fuller review would come back to the July 2020 ARC meeting.	Lisa Cherry	July 2020 ARC meeting	A paper will be presented to the July ARC meeting.	OPEN
6. Annual Legal Risk Report 2019/2020					
6.	It was noted that we were putting in place a due diligence approach with our key partners, including where we might need to trigger a force majeure clause; this would be circulated to the ARC when finalised.	Sherrill Taggart	19 May 2020 ARC Meeting	A due diligence review of the PO top 24 material supplier and client contracts was undertaken to understand the exposure under the contracts - this will include reviewing the existence and terms of any force majeure provisions, considering any other relevant provisions such as clauses around termination generally, price adjustment, variation, material adverse change, limitation of liability, remedies, business continuity, disaster recovery and dispute resolution. In addition, training, guidance notes and template documentation have been rolled out to the contract owners and contract managers of the top 24 material contracts to support them in the management of their contracts.	**Recommended for closure**
6.	Bring a revised plan to the next ARC meeting setting out how we were going to bridge any gaps in contract management. The focus on the top 15-30 contracts would help us understand where we had any issues with those contracts or the management of those relationships.	Sherrill Taggart	19 May 2020 ARC Meeting	This is included in the Contract Management Framework Update.	**Recommended for closure**
7. 2020/21 Internal Audit Plan					
7.	We needed a revised plan that reflected the current environment and the top five priorities. We also needed a monthly update from Deloitte on the external environment, including risks and the approach other companies were taking to managing their risks and running their businesses	Johann Appel/ Deloitte		Ongoing. Deloitte will provide a monthly update to the ARC.	OPEN

POL00401577

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 12 May 2020

7.	Johann Appel would circulate a revised plan in advance of the next ARC meeting	Johann Appel	19 May 2020 ARC Meeting	Prepared an updated plan, which Johann will share with Nick and then will circulate it back to the ARC. This is included in the May ARC pack.	**Recommended for closure**
10. Contract Management Framework Update					
10.	**AGREED** that a paper should be brought back to the next ARC meeting with a dashboard for the material contracts, the contract owner, which contracts were missing, which had been loaded to S2S and which contracts were due for renewal in next 18 months or so.	Sherrill Taggart	19 May 2020 ARC Meeting	Sherrill has set up the contract management training. The recommendation to the ARC is for the implementation of the CMF to be completed for all contracts identified by GE and GE-1 as being material to the Post Office Group, in terms of strategic and financial value. The annexes included in the associated May ARC paper include a list of material contracts for which the project team has not, as yet, been able to locate contracts for and those material contracts which have already been uploaded onto Web 3.0, with their obligations mapped. Given the project seeks to complete the implementation for all material contracts, and is confident of doing so, renewal dates are not provided – although these will be uploaded onto Web 3.0.	**Recommended for closure**
11. Managing Procurement Relationships					
11.	It was **AGREED** that Al Cameron would convey the ARC's views to the GE and that a paper would be provided for Board on 8th April 2020.	Al Cameron	8 April 2020 Board Meeting	Barbara and Al have produced and presented the Procurement/ PCR paper for Board on 8th April 2020.	**Recommended for closure**
12. Selling Regulated Products in the Branch Network					
12.	Mails Dangerous Goods compliance: It was **AGREED** that an action plan would be created and provided as part of the next Compliance Report to the ARC.	Amanda Jones/ Andy Kingham	19 May 2020 ARC Meeting	An update on Dangerous Mails Action plan is provided as part of the May Compliance Report.	**Recommended for closure**
13. PCI-DSS and Cyber Security Update					
13.1	ARC had requested regular confirmation in writing from the Fujitsu and Ingenico CEOs that work was on track from their side. Jeff Smyth would respond to the ARC on what we could put in place and the time period for reporting adherence to timelines	Jeff Smyth		We now have monthly CEO-CEO session in place with Nick Read and his counterpart at Ingenico (Dan Martensson) where implementation progress is reported and reviewed. Fujitsu report their monthly progress on PCI-DSS deliverables via Steer-Co and Nick has periodic review sessions with Paul Patterson (Fujitsu, Head of Sales & UK County Leadership)	**Recommended for closure**
15. Audit Update					
15.	Al Cameron reported that Traction software for monitoring internal controls supported by PWC was used	Mark Baldock	19 May 2020 ARC Meeting	An update on the move to Archer is provided in the May Risk Report.	**Recommended**

POL00401577

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 12 May 2020

	widely in the organisation and that, due to limitations on services that can be provided by external auditors, we needed to move off this system. The plan was to move everything onto Archer after testing migration issues. Mark Baldock would report on the progress of this work in the next Risk report				**for closure**
28 January 2020					
4. PCI-DSS and Cyber Security					
4.3	The Committee urged the management team to press for compliance pre-Christmas, even if roll out was delayed until after the Christmas trading period. He did feel more assured with the joint effort/approach to compliance.	NR	March	Further CEO level talks are expected to take place in April 2020.	Open
4.4	It was **AGREED** monthly progress reports (signed by Ingenico's CEO) would be provided to the Committee.	JS	On going	This has been agreed by Ingenico, to commence circulation.	Open
4.7	TJ presented an update on Cyber Security. Following the Travelex ransomware attack, focus had been on reviewing and strengthening cyber defences where required (considered suitable at present). A verbal update had been received from FRES that their systems are suitable. A more formal confirmation is due in 2 weeks. Following a question from the Committee, it was confirmed that POI is included in the POL work, but Payzone have yet to be tested.	TJ	March	Formal confirmation has now been received from FRES indicating that systems are suitable.	**Recommended for closure**
4.8	**Cyber Security - Joiners, movers, leavers** Regarding JML (joiners, movers, leavers), TJ had a good understanding of the processes involved and a plan would be rolled out in March to ensure accessibility rights was continually managed. Currently there was a good	TJ	March	A plan has been presented in the Cyber Security update paper.	**Recommended for closure**

POL00401577

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 12 May 2020

	basic coverage but some slippage occurs. There are currently 90 contractors in POL, 235 at its peak in October 2018**. A full plan on JML will be shared with the ARC at the next meeting.**				
11.9	Updated guidance by the regulator (ICO) clarified the use of management of cookies on websites. POL is now non-compliant against regulation and work is underway to develop solutions for mitigation. It should be noted that all solutions will impact on POL's use of marketing data. The Committee requested this be kept under review.	JH	March	An update on this can be found in the Compliance report.	**Recommended for closure**
11.11	GDPR/Contracts Governance It was AGREED that an update on non-compliant contracts would be presented to ARC every quarter.	DP	March	A paper is being presented in this pack on procurement compliance.	**Recommended for closure**
25 November 2019					
5. Contract Management					
5.3	BF to review and present Top 50 contracts i.e. those with the greatest financial and strategic value.	BF	March 2020	~~Under review and on train.~~ An update paper is being presented this month.	**Recommended for closure**
5.3	MB/NR That the full accountability matrix based on the RACI principles should be compiled and presented to the Committee. It was discussed and agreed that this should be extended to all functions (not just contract management). The Operational Risk team will assist NR.	MB/NR	March 2020	An updated matrix will be presented once NR confirms his new management structure and accountabilities. Central Risk have refreshed the Post Office enterprise risks such that there are now 14 enterprise risks and 55 linked intermediate business risks. Each of these risks has a designated GE or GE-1 owner in line with the latest Post Office organisational structure. Ownership will be change controlled as individual risks emerge, are managed and then recede. Specific ownership will be included as part of the Archer Dashboard reporting suite going forward.	Open
5.3	Auditors to provide examples of best practice for contracts management.		March 2020		Open
7. Commercial Partner Contingency Paper (McColls)					

POL00401577

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 12 May 2020

7.5	An update paper on how POL would de-risk itself over the next 3 years. Whether a strategic review to cap partner estates (to reduce the risk and impact on POL) should be completed by the POL Board.	AJ	March 2020	An update paper is being presented in this meeting.	**Recommended for closure**
23 September 2019					
5. PCI-DSS					
5.6	NR to hold talks with CEO of Ingenico to progress PCI compliance.	**NR**	November	There has been a change in leadership at Ingenico. Shikha Hornsey to provide further details in PCI-Compliance update. NR spoken to Ingenico on 17 December 2019.	Recommend for closure.
5.6	TC to hold talks with his French counterparts to progress PCI compliance	**TC**	November		Recommend for closure.
5.6	An update on PCI compliance including commercial figures would be presented at the October Board meeting.	**SH**	October	There has been a change in leadership at Ingenico. Shikha Hornsey to provide further details in PCI-Compliance update.	Recommend for closure.
6. Transformation Office Changes					
6.5	Consider the prioritisation of the change portfolio at the POL Board	**DZ**	January 2020	To be included in January Board agenda.	Open
29 January 2019					
6. Money Laundering Reporting Officer (MLRO) Annual Report					
6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	**Nick Boden/ Sally Smith**	Ongoing	**Ongoing until project close.** Item included on ARC agenda.	Open
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	**Rob Houghton / Mick Mitchell**	May 2019	**Ongoing.** Item included on ARC forward agenda.	Open
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	**Exec**	~~May 2019~~ July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open

POL00401577

5.3

POST OFFICE LIMITED
RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance Committee ("RCC") meeting held via Microsoft Teams
on 06 May 2020 at 14:00

Present:	Alisdair Cameron (Chair) (AC)	Group Chief Financial Officer	
	Ben Foat (BF)	Group General Counsel	
	Amanda Jones (AJ)	Group Retail and Franchise Network Director, Interim	
	Lisa Cherry (LC)	Group Chief People Officer.	
	Jeff Smyth (JS)	Group Chief Information Officer, Interim	
	Julie Thomas (JT)	Operations Director	
	Andrew Goddard (AG)	Payment Propositions Director (deputising for Owen Woodley)	
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	
	Rebecca Whibley (RW)	Assistant Company Secretary	
	Tony Jowett (TJ)	Chief Information Security Officer	Item 5
	Sherrill Taggart (ST)	Legal Director, Interim	Items 6 & 7
	Barbara Brannon (BB)	Procurement Director	Item 8
	Rod Williams (RW)	Head of Legal, Dispute Resolution & Brand	Item 9
Apologies	Nick Read, Group CEO		
	Owen Woodley, Group Chief Commercial Officer		

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

1.1 The Chair opened the meeting and advised that all papers would be taken as read. No conflicts of interest were declared.
AC noted there were four issues that were being managed under legal supervision and which would be discussed at ARC:

1. An independent review of suspense accounts as part of the GLO work;
2. An independent review on stamps and whether there were GLO implications;
3. A CBRE performance issue that had been uncovered; and
4. Work ongoing to validate historical final salaries for the defined benefit pension scheme.

2. Minutes and Action Lists

2.1 The minutes of the RCC meeting held 9 March 2020 were **APPROVED**.

2.2 Progress on completion of actions as shown on the action log was **NOTED** and the actions assigned to SH (Shikha Hornsey) were to be reassigned to JS. The following action updates were provided: **To do: RW**

- Action 3.3 from 14 March 2020 relating to FRES Audit would be completed before the next RCC and the action remained **open**.
- Action 3.3 from 4 March 2020 relating to guidance from the National Cyber Security Centre was **closed**, the guidance having been shared with the Group Executive (GE) and Board.
- Action 4.12 from 14 March relating to the Ofcom Information Requests was **closed**.
- Action 6.6 from 14 March relating to the issues being flagged to the RCC or ARC was questioned as to its context and it was requested that more information was provided as it was not enough to simply say that it was not raised. The action remained **open**. **RW**
- Action 6.18 from 14 January 2020 relating to Payment Services Directive was **closed**.
- Action 10.6 from 14 January 2020 relating to Money Laundering Reporting Officer (MLRO) Annual Report had been delayed due to scheduled meetings being postponed. The action remained **open**.
- Action 3.2 from 7 November 2019 relating to supplier contracts out of governance (SSK) remained **open**.
- Action 3.3 from 7 November 2019 relating to supplier contracts out of governance (Brands/RAPP) remained **open**.

POL00401577

- Action 4.1 from 7 November 2019 relating to the PCI-DSS Update and final pricing deadlines from Ingencio was **closed** as this item had become a regular RCC agenda item. **JS**
- Action 5.3 from 7 November 2019 relating to major incident testing remained **open** and JS advised he would obtain an update.
- Action 5.3 from 7 November 2019 relating to Joiners/Movers/Leavers and third party access remained **open** and TS was asked to provide an update.
- The following actions from 7 November 2019 were otherwise **closed**: 5.3 Cyber Security relating to Joiners/movers/leavers and the contract review, 5.3 Cyber Security relating to Joiners/movers/leavers being added to the Internal Audit Plan,6.14 relating to Data and Analytics Excellence (Programme Assurance) and 7.5 relating to Contracts Management Framework.
- Action 5 from 7 November 2019 relating to GDPR was **closed** as JH advised that contracts had been identified and the GDPR programme was due to be completed at the end of June 2020.

5.3

3. Combined Risk, Compliance and Audit Update

Risk

3.1 MB explained that since the last RCC on 14 March 2020, his team's focus has been on the COVID-19 crisis and fortnightly risk updates were being provided to the COVID-19 SteerCo, which was included in the paper to the RCC. This work had been undertaken in two phases. The first was to undertake the industry-wide and sectorial analysis of the typical emerging COVID-19 risks and was completed by 31 March 2020. The second phase was to discuss the risks that had been identified with the business to confirm relevance and to assess their respective impacts, likelihood and proximity. It was concluded that there was one single overarching COVID-19 enterprise risk, 13 intermediate thematic risks (operational, strategy, legal, financial etc.) and 56 specific low level risks. One major risk was having insufficient change funding available to deliver planned change activity and it as noted that this was due to be discussed at the Board.

3.2 Work was now moving to merge existing risk work with the COVID-19 risks due to the wide scope of these risks. The team was also continuing to implement Archer and MB explained that all risks were due to be entered into Archer by the end of next week (15 May 2020) and the system was to be rolled out to the wider business from 31 May 2020.

3.3 MB also highlighted that his team had produced a risk appetite statement for COVID-19, but that this had evolved into a wider enterprise risk statement and he would be requesting that this statement be considered at the GE in June 2020 (MB to request a GE agenda slot with Veronica Branton, Company Secretary). **MB**

Compliance

3.4 **Telecoms**: JH noted that the regulators have indicated they would not be stepping back from compliance but were being more understanding on the timing for compliance. As an update to the paper, JH explained that his team were now required to provide a weekly update to Ofcom as to our COVID-19 response and they have indicated they are happy with our progress as we are able to do the end of contract notifications, which other providers are still having issues with. Further, we have also just signed up to the Department of Culture, Media and Sport's (DCMS) commitments, including free and low cost calls for vulnerable customers, working with customers who may be struggling with debt and removal of data caps. A statement via DCMS would be released over the weekend. In response to a question from the Chair, JH and AG confirmed (having checked with Meredith Sharples) that there was no financial impact arising from vulnerable customers being unable to pay their bill.

3.5 **PSD2**: JH explained that Fujitsu had now confirmed that they will put in place a fully compliant solution but this would not be the most expensive solution by the beginning of August 2020. There would be a minimal increase in cost, but this was a regulatory requirement. Once in place, we could then apply for an Electronic Communications Exemption (ECE), although we were not being chased to do this.

3.6 **European Electronic Communications Code (EECC)**: JH noted that this would impose new regulatory obligations on all providers. It presented a big challenge for Post Office and had cost implications. Clarity as to what was required was expected from Ofcom but that the DCMS has indicated that it expected providers to meet the implementation deadline of 21 December 2020. The concern was that any clarity from Ofcom may come after this deadline, but it was hoped there may be some leeway. Al noted that if clarity was not forthcoming, we could approach the Department of Business, Energy and Industrial Strategy (BEIS) to support us in seeking this clarity and/or asking for leeway on the implementation deadline. It was also noted that similar changes made to the switching process in the energy industry by Ofgem had led to less switching of providers by customer and therefore there could be retention opportunities for Post Office.

POL00401577

3.7 **Branch Registration Fees:** JH explained that Her Majesty's Revenue and Customs (HMRC) have confirmed that we could defer payment for Branch Registration fees (amounting to circa IRRELEVANT until 1 December 2020 (from 30 June 2020). However they have advised that they would calculate the fee based on the June branch data, rather than the December data. This does not go far enough and we would continue to lobby against the decision via BEIS, Her Majesty's Treasury (HMT) and HMRC directly to get HMRC to allow the calculation to apply from 1 December 2020. It was hoped that a positive response would be received soon.

3.8 **Cookies**: JH confirmed he was speaking to Henk van Hulle to try and achieve quicker and cheaper compliance.

3.9 **Belfast Data Centre Exist and move to the Cloud**: The Chair questioned who was having the client conversations and it was highlighted that there should be engagement with client management owners. JH was asked to pick this up with the Commercial team and JS was asked to check with the IT Project Team. **JH/JS**

3.10 **Whistleblowing**: The Chair asked that he was provided with information as to the kind of issues that were being raised by whistleblowers, insofar as it would not breach any confidences. He also questioned whether it was appropriate to be putting investigations on hold. JH explained that these investigations had been put on hold as they required the physical movement of people which was not possible during lockdown. The Chair requested that the investigations were reviewed on a case-by-case basis with HR and challenge the assumption that the investigation had to be paused. If a major issue was subject to the complaint, the response needed to be balanced. **JH** **JH**

3.11 **External Threats – Lottery:** The Chair questioned the wording regarding the Post Office provision of the Lottery having been previously assessed as low risk and JH confirmed that it had been assessed and no issues had been identified. Payzone services were yet to be assessed but AG explained that he did not view it as high risk. The wording of the section would be reviewed before submission to the Audit, Risk and Compliance Committee (ARC) so that it was clearer. **JH**

3.12 **Dangerous Goods**: The Chair noted that overall performance for P12 had dropped to 46% and therefore had got worse. However the Voice of the Customer survey suggested that the question was being asked 75% of the time. IT was noted that the Board may be concerned about the risk of low compliance in this area. Amanda explained that a project had been initiated to place the onus on the customer to confirm what was in their parcel via a validation on the Pin Pad (to reflect the SSK process). The Chair requested that this section of the paper be updated prior to submission to the ARC to better outline this project. **JH/AJ**

Internal Audit

3.13 **2019/20 plan progress**: JA explained that the completion of the 2019/20 internal audit programme has progressed well, however, the final five reviews (three in Post Office and two in Post Office Insurance) 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 awaiting management comment. These related to branch sales which had been given a "needs improvement" rating, but the issues raised were not contentious and savings products, which has been given a "green" rating. AG was asked to chase the Commercial Team to ensure that management comment was provided as soon as possible to enable the complete reports to be ready for the ARC on 19 May 2020. Otherwise, the 2019/20 plan was complete (except for the reviews postponed due to COVID-19). **AG**

3.14 **2020/21 plan progress:** JA explained that the plan was due to be approved by the ARC on 19 May 2020 but in the meantime, three of the top five reviews had been started: COVID-19 Assurance Programme, Maintain Minimum Control Standards and Cyber Security Maturity.

3.15 **Internal Audit reviews completed**: JA noted that the outcomes of the three final reviews:

- Postmaster on-boarding: This was rated as satisfactory and the new process was deemed effective with recommendations from GLO having been implemented.
- Vetting and Fit & Proper: This was rated as needs improvement due to the very fragmented processes that were in place and the lack of clear ownership. Fit & Proper was slightly better than vetting and improvement on vetting was expected when the ownership issues were resolved. It was explained that accountability had been split between the Operations team, HR and Compliance. It has been agreed to bring accountability into the Operations team within clear oversight from Compliance. The Fit & Proper policy was also being updated and LC was asked to ensure that HR were involved in this update. JH confirmed he had a new Vetting and Oversight Assurance Manager starting on 11 May 2020. **LC**
- Change Control Framework: This was rated as needs improvement. The Chair noted that he felt elements of the report were confusing and needed to be clearer. JA explained that this was a follow up review following a review last year which looked at gating, benefit realisation and second line assurance activity and outlined the need to establish a control framework for change activity.

POL00401577

The purpose of the present review had been to assess to what extent the previous recommendations had been implemented. It was noted that most findings had arisen from the self-assessment process (the Strategic Portfolio Office (SPO) had been quite conservative in its ratings) and that 29 out of 29 controls were assessed as partly effective. This sounded more serious that it was because this rating had been given if only one programme in the test had failed. JA was asked to ensure this context was clearer in the report. **JA**

3.16 **Status of Audit Actions**: JA noted that five actions were due at the end of April which had been harder to close due to other priorities relating to COVID-19. Some actions may need to be extended but any extensions would be agreed prior to the ARC on 19 May 2020. AG requested that JA send him any outstanding actions relating to the Commercial Team. **To do: JA**

3.17 Subject to the amendments as outlined, the Combined Risk, Compliance and Audit Update was **NOTED for onward submission to the ARC**.

5.3

4. Internal Audit Plan

4.1 JA explained that audit plans had become dynamic against moving targets due to the COVID-19 crisis and that he has been webinars with other heads of audit. This has shown that the Post Office approach has been similar to other organisations and a key element was that there may need to be some compromise on the maintenance of controls during the COVID-19 crisis. The top five priorities were outlined as:

- COVID-19 Programme Assurance/Support;
- Maintain Minimum Control Standards;
- Cyber Security Maturity;
- Health & Safety response to COVID-19 crisis; and
- Effectiveness of Second Line during COVID-19.

4.2 The medium priority reviews were outlined as:

- GLO Operations Improvement Programme;
- Postmaster Reporting;
- BCP Post-crisis assessment;
- Branch Hub; and
- Stamp Stock (relating to inventory controls).

BF noted that it would be helpful to have an external view of Stamp Stock and it was agreed that BF and JA would pick this up. JA explained that his internal review would only take place after the external review into stamps and whether management had led to systemic agent losses. Similarly the review into the GLO Operations Improvement Programme would be done after the planned external GLO response review. It was noted that this was a case of timing and consideration as to whether an end-to-end external review was required as the Norton Rose review was simply a gap analysis. JA was asked to look at this in conjunction with BF and JT. Regarding the COVID-19 Assurance Programme, MB questioned whether this would extend to the scope of Project Neo and risk and JA explained that this was not presently included but that he would discuss with MB. JA further noted that he had issued an interim report to Caroline Scott on the review of phase 1 of the COVID-19 Programme. In response to a questions from AJ regarding Postmaster Reporting, JA confirmed that he would discuss the scope of the review with her and her team nearer to Q3. **JA/BF** **JA/BF/JT** **JA/MB**

4.3 The Internal Audit plan, including the internal audit priorities during the COVID-19 crisis, was **NOTED for onward submission to the ARC.**

5. PCI-DSS and Cyber Security Update

PCI-DSS Programme Update

5.1 **Ingencio CEO call**: JS explained that CEO to CEO dialogue between Ingencio and Post Office had been established as requested by the ARC and there was diarised meetings between the Global Vice President of Ingencio for retail and banking and Nick Read. Written reports from the calls were provided to JS. It was noted that Ingencio were not reporting any direct implications for their services owning to COVID-19 at present.

5.2 **Integrated Programme Plan:** It was expected that the programme would obtain Ingenico final banking software deliverables in early February 2021 and branch rollout would commence in late March 2021. Branch rollout would be completed in May 2021 and formal PCI-DSS accreditation would be achieved by June 2021. The team has also held a deep dive into the plan itself and work was ongoing to see if the delivery plan timeline could be improved further. The business case for IRRELEVANT would be presented to the Investment Committee and Board in May.

POL00401577

5.3 **PED rollout programme:** JS noted that this programme was presently on pause due to the COVID-19 crisis and the present thinking was that this would recommence in July, subject to the Government announcement on lockdown expected on 10 May 2020.

5.4 IRRELEVANT JS noted that most other organisations were compliant but that there had been some delays with IRRELEVANT The Chair questioned whether Post Office would have any recourse if IRRELEVANT IRRELEVANT JS explained that the target operating model included the ability to pay Santander IRRELEVANT ut at present, we were not setting out to utilise this. The issues IRRELEVANT re facing seemed genuine and Nick Read had already been on a series of calls to try to resolve.

5.5 The PCI-DSS Programme Update was **NOTED for onward submission to the ARC.**

Cyber Security

5.6 **Cyber Security Maturity**: TJ outlined that the maturity score was averaging 2.4 in mid-April and he hoped this would improve to 2.45. This figure was an estimate and it would be retested by Deloitte and Jonathan Acres from Post Office from 11 May 2020. This retest would allow the reassessment target maturity due to recent events. A new change programme was being developed to close any gaps identified and an update would be provided to the next RCC.

5.3

5.7 **COVID-19 risk, issues and threats:** The team has been working with Data Protection and IT Operations to enable people to work from home, but they were also ensuring that any exemptions to our usual policies were being closed down rapidly. Data loss was also being monitored, although a slightly softer approach was being taken to enable home working. Work had also been completed to ensure the IT Service desk can communicate with colleagues securely. It was noted that the team was feeding into and monitoring the National Cyber Security Centre's (NCSC) work on COVID-19 threats. The mains threats were fake Post Office websites and phishing. During the COVID-19 crisis, security threat activity was up between 25% and 55% depending on the type of activity which included money miles and password attacks.

5.8 **Social media presence**: TJ outlined that in response to the RCC action the guidance on protecting ourselves on social media had been shared with the Board and GE. Links to the guidance were available in the paper.

5.9 The Chair requested that a more extensive update on the Joiners/movers/leavers programme was included in the paper for the ARC on 19 May 2020 and that a draft should be reviewed by the Chair. **TJ**

Subject to the amendment as outlined, the Cyber Security Update was **NOTED for onward submission to the ARC.**

6. Progress Update on the Pilot Implementation of the Contract Management Framework

6.1 BF explained that 142 top material contracts had been identified. By the end of the pilot (19 May 2020), it was expected that 60 material contracts would have been uploaded to Web3.0 having had their obligations mapped at a cost of IRRELEVANT he balance of 82 material contracts would take a further month to upload at an additional cost of IRRELEVANT here were also 1,500 other contracts which have not been uploaded to Web3.0 and had their obligations mapped. It was recommended that due to the current commercial environment, the pilot should work to complete the upload and mapping of obligations for the top 142 material contracts but that the other contracts should not be uploaded as part of the pilot and should be uploaded during the natural contract lifecycle (as amendments or extensions arise). It was proposed that the accredited external training which had been budgeted for at a cost of IRRELEVANT was not pursued, releasing this money back to the business and for IRRELEVANT o be reallocated to support the mapping of the outstanding material contracts. The Chair requested that BF discuss the approach with Carla Stent, ARC Chair, prior to submitting the paper to the ARC to get a steer as to whether this approach would be acceptable. **BF**

The RCC NOTED the paper and APPROVED the following for onward submission to the ARC, subject to BF gaining steer from the ARC Chair as to whether this approach was acceptable:

- 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 IRRELEVANT of the IRRELEVANT 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 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 IRRELEVANT rom the 20/21 Change Portfolio Budget.

POL00401577

7. Horizon Scanning Update

7.1 BF explained that this was a new report for the RCC and had been presented to assist in the enhance of the legal maturity of Post Office by ensuring that the Board and Executive team were proactively managing legal and regulatory risks as they develop. This was supplemented by regular Law In Trends forums which were cross-functional and looked a legal and regulatory changes on the horizon and discussed how Post Office might need to respond. The Chair complimented the paper and BF confirmed that the paper would be developed over time to include a Red/Amber/Green (RAG) status against each element.
The Horizon Scanning Update was **NOTED for onward submission to the ARC.**

8. Supplier Contract out of Governance

8.1 BB explained that there were no contracts out of Governance that required approval as all approvals had been addressed at the Board on 8 April 2020. The Chair requested that the paper be reorganised to cover new requests first, then any future contracts on the horizon and then any past approvals. **BB**

5.3

8.2 On the future contracts that were high value and at risk of being awarded or extended non-compliantly, BB outlined the following:

- End User Computer services (EUC) (value of £10m): Discussions were still being held between IT and the Change project team as to whether there would be sufficient funding to run a procurement. A paper regarding this project was being prepared for the GE on 13 May 2020.
- Common Digital Platform (CPD) (value of £5m): There was an option for a six month extension to December 2020 on a short term basis to allow for cloud migration and long term strategy adoption. This was already being discussed with the supplier to enable an extension whilst a procurement process is run.
- Brands/Rapp (value of £1.3m): The sourcing process has not been agreed with the business and their appetite to migrate the service was limited. Funding was also an issue.
- ATM support (value £350,000): There were a number of contracts expiring in August 2020 which may need to be extended non-compliantly whilst the tender process continued.
- Identity Services (value of £5m): A full sourcing plan has been agreed to be funded out of OPEX Identity budget, but this has been derailed by the COVID-19 crisis. Discussions were ongoing between Martin Edwards, Digidentity and Legal to ensure extension to March 2021 which would give more latitude to manage the OJEU required and would give the business more time to review other options. In the interim, discussions were ongoing with the Commercial team as to whether our approach needed to be changed given COVID-19 crisis.

It was further noted that otherwise the procurement pipeline was very quiet. This was thought be to because feedback had gone to the business explaining that risks would not be excepted and because of the spending freeze.

8.3 Subject to the outlined amendments, the Supplier Contracts out of Governance Update was **NOTED for onward submission to the ARC.**

9. Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct Policy

9.1 BF explained that this was a policy to cover how Post Office dealt with suspected criminal misconduct covering private prosecutions and cooperation with third party law enforcement agencies, regulators and industry accredited bodies. The policy sought to balance the following risks: safeguarding the integrity of HNG-A so that it is not unnecessarily undermined or brought into question without the proper governance around the release of information against being seen to support and cooperate with law enforcement agencies. The approach would be that we would support third parties to investigate criminal misconduct if there were mandatory requirements. Where it was not mandatory, we could exercise discretion as to whether to assist but it was a question of who within the business would have the authority to authorise the release of information. We have taken risk based approach: where the data would not rely solely on integrity of the Horizon system (i.e. other evidence such as CCTV existed), and therefore the integrity of HNG-A was unlikely to be brought into question, we would provide the data to the requesting body. BF further outlined that there was a risk with the policy in that it could not prevent potential law enforcement proceedings if they struck at the heart of the Horizon system and this could mean that the integrity of the current Horizon system was called into question. Therefore work still needed to be done with IT to be able to substantiate that there were no known bugs and this needed to become a BAU process.

9.2 BF noted that the team would undertake an "optical review" of the policy before it was presented to the ARC. This was because, although such documents would not usually be discoverable, it could do so in the future. As such the policy needed to be reviewed to consider how it may be viewed by the public. BF further outlined that the policy would prohibit Post Office from engaging in private prosecutions without the

POL00401577

express consent of the Board. It was also noted that any data provided from legacy or HNG-X Horizon would be provided with a health warning given the findings of the Horizon judgment.

9.3 JS cautioned that there would be a cost to operationalise this policy as a process would need to be in place to deal with any approaches from law enforcement agencies, regulators or registered industry bodies. We needed to ensure that we had the skills, capacity and money to deliver. BF explained that the policy included a process map but that he would highlight this at GE to ensure that the consequences of the policy were understood. **BF**

9.4 It was further noted that requests for data may not be easy to fulfil if it required cooperation from third parties including Fujitsu and Ingenico. JS explained that it needed to be recognised that this involved some very comprehensive relationships. BF concurred but noted that this would be mitigated by general law cooperation clauses within contracts. AG noted that the paper was very "Horizon-specific" but that the policy had a much broader systems reach. BF explained that the policy was designed to cover all requests, but that HNG-A was an area of particular sensitivity. It would be supported by a cross-functional team including compliance and IT security. As such, support would be provided to the business. JT suggested that a list should be compiled of colleagues who could provide information to law enforcement agencies, regulators and industry bodies to ensure compliance.

9.5 The Criminal Misconduct and Cooperation with Law Enforcement Agencies paper and attached draft policy entitled "Cooperation with Law Enforcement Agencies and Addressing Suspected Criminal Misconduct" was **APPROVED for onward submission to the ARC**. In approving the draft policy, the RCC also:

- decided that Post Office's policy should 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;
- approved, 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);
- decided that Post Office's policy should be not to conduct any private prosecutions at present; and
- decided that 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.

10. Review of draft Audit, Risk and Compliance Committee meeting agenda for 19 May 2020

The draft ARC agenda for 19 March was **NOTED** and RW was requested to confirm with Carla Stent (ARC Chair) and JS the scope of the "broader Fujitsu update" and to add a noting paper for the Supplier Contracts out of Governance update. **To do: RW**

11. Any other Business

There was no other business.

DRAFT

POL00401577

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE

Title:	POI Risk and Compliance Update	**Meeting Date:**	19 May 2020
Author:	Ian Holloway, POI Director of Risk and Compliance	**Sponsor:**	Amanda Bowe, Chair of the POI ARC

Input Sought: Noting

The report is provided for information and discussion.

Previous Governance Oversight

Not applicable as there is a direct line of reporting from the POI ARC to the Group ARC.

7

Executive Summary

In the current Covid-19 environment POI Management are most concerned with maintaining good outcomes for our customers. POI has flexed the way it operates its products, notably by allowing full refunds for travel business outside of the statutory period, and by offering flexibility on household and motor products where customers find they are working more from home, or travelling to differing places of work as a result of the Covid-19 emergency.

POI is considering in conjunction with its partners how it operates forbearance, where credit has been provided for motor and household cover. This follows FCA draft guidance. Under review is the length of any payment holiday (1-3 months), to what level we might waive interest and how products might be adjusted to meet customer needs.

The travel product remains suspended, given it cannot provide effective benefits in an environment where travel is not possible. The loss of travel is significant to POI as it is the major cash provider within the business. Action is required to effectively manage cash flow over the next two quarters.

Recessionary pressure is also a significant concern with a consequent potential sales and profitability impact.

POI notes the importance of effectively monitoring third parties during the current crisis and also of the quality of the relaunch plans for travel and protection in the coming months.

The Nemesis project has been successfully completed in the course of the lockdown.

Appendix A summarises POI's approach to Risk Management.

Questions addressed

1. What are the current proximate risks within the Covid-19 environment which POI is most concerned with?

Report

POL00401577

What are the current proximate risks within the Covid-19 environment which POI is most concerned with?

1. The current Covid-19 crisis has fundamentally impacted the POI business. Travel business (our largest product), was taken off sale on March 15 2020, given government advice not to travel abroad. Sales of protection business which have strong links to the branch network, have also been very significantly impacted. In the light of this impact, a risk analysis was prepared for the POI ARC meeting on 14 May 2020 which focused on the proximate Covid-19 risks and potential mitigants. It also focuses on the risks that POI is likely to face shortly after the current lockdown has finished. The full risk paper has been placed in the reading room.

2. Informed by our customer and regulatory risk appetites, customer focus has been at the centre of POI's post Covid-19 response. In particular:

3. **Product** - As noted above, the POI travel product was suspended, given Management did not believe that sufficient value could be offered given a Covid exclusion. POI are working with underwriters to ensure that a product can be developed which will provide Covid cover. These discussions are well advanced, and it is hoped that POI will have a product ready for launch within the coming month. POI has also proactively reviewed its wider product set to ensure it continues to provide appropriate value to customers in areas such as HEC and protection. Our conclusion is that value is appropriate.

4. Management have considered the current moratorium on our over 50s product which significantly restricts the pay out to customers if the customer dies within one year of policy inception. This restriction is clear to customers at the point of sale, and it is unlikely to be possible to remove this restriction without significantly increasing the premium.

5. **Flexibility -** POI has already adopted flexibility in the cancellation of travel insurance products. Where customers have not made a claim we have allowed cancellations for free outside of the normal statutory period. In line with FCA guidance, POI is also maintaining cover, where a customer's policy is due for renewal prior to a pre-booked holiday.

6. **Forbearance** - FCA has produced draft guidance on forbearance. FCA looks for firms to consider interest waivers and payment holidays of up to three months. This is to provide support to customers who are experiencing short term difficulty. For POI this is relevant to our GI business areas (motor and household), and we are working with our partners to define how this guidance might be implemented. Currently our partner BGL (for motor), does provide up to three months relief. Premium Credit Limited (PCL- who provide credit for household), provide one month and are considering if this can be increased. Practice across the industry has varied. A number of insurers such as Aviva and AXA have voluntarily offered three months forbearance prior to FCA output. Brokers operating panel arrangements have generally not offered the same arrangements, given their greater dependence on premium finance income.

7. For both motor and household, we are currently considering how we could meet FCA requirements to adjust products to meet the short term needs of customers, though across the industry there is a view that this will be challenging without giving advice, and without providing some form of detriment. For example, if an excess is increased than this may increase the financial pressure on customers should they then have to make a claim.

POL00401577

8. **Premium refunds** - The Committee will note that some firms have been providing premium refunds to customers for motor business on the grounds that motor claims are likely to be lower. Again practice across the industry is mixed with Admiral and LV offering limited refunds (though to only direct customers), whilst other large players have not. We are however aware that discussions are ongoing and this position may change. At this stage POI would plan to focus on working with motor insurers to deliver the keenest new business and renewal prices to customers on the grounds that this is likely to lead to the best customer outcome, rather than a token refund gesture.

9. The highest graded risks identified within the POI analysis were:

10. **Our travel insurance business does not recover over the next twelve months with a consequent impact on cash flow**. Significant uncertainty remains. However in the view of Risk, there is a high risk of crystallisation within the second quarter of 2020. A number of activities are currently under way to manage cash flow, including action on commission levels paid to POL and further cost containment. However, without further action, cash flow is likely to be an issue in the second quarter of 2020/2021.

11. **POI needs to write down all or a portion of the Goodwill on the balance sheet.** This development will not have an impact on cash flow and the need for a write down is still being discussed with our auditors. In essence, if the carrying of goodwill cannot be supported by the ongoing prospects of the business, it will need to be written down with a one-off impact on the profit and loss account.

12. **Recessionary pressure impacts business across all channels.** Most economic commentators expect the Covid-19 crisis to lead to a significant recession with significant unemployment (the OBR estimates c.10%), a contracting economy (2-15% is forecast over the coming half year by the OECD), and housing market falls of up between 5 and 20% (forecast by Barclays). The direct impact on POI is difficult to estimate, and on areas such as travel, a recessionary impact has been built into our business planning. However, Management remain conscious that the likely recession has the ability to impact significantly on our business.

13. A number of other important risks fall slightly below this level but remain important. In particular Management note the risks relating to overseeing our key third parties, both in terms of managing service levels and in ensuring that they remain financially sound. All POI staff, and the staff at our third party call centres are now home based, and oversight processes are performing well.

14. POI has been heavily focused on the monitoring of service standards and sales quality, particularly during current periods of volatility. Webhelp did experience some issues with maintaining service in March, given very high web traffic caused the service to crash on a number of occasions. However, services have been maintained at an adequate level, and limited complaints have been received. BGL are for the moment only supplying enterprise level data, i.e. not specific to POI. We have noted our concerns with this, but following the furloughing of staff, this position is unlikely to reverse in the short term.

15. POI has also been active in working with underwriters to ensure that their service levels remain adequate. Travel insurers have prioritised emergency medical claims, and have noted an increased level of declinature given the large numbers of customers who are cancelling holidays. However, in our view service levels have remained adequate over this period.

POL00401577

16. Management are also aware that the quality of the strategy for relaunching travel and for developing our protection are key to sustaining the viability of our business over the next six months, and significant focus on these areas is required.

17. The importance of managing an excellent relationship with POL should also be noted, particularly around gaining appropriate branch focus on the protection strategy and supporting the relaunch of travel within the network when this is possible.

18. Between now and the end of the year, POI will also face a number of other potential tailwinds to business performance. Notably the risks posed by Brexit and the FCA's ongoing work on differential pricing. The management of these risks may impact on POI's business plans and may require significant Management time.

19. Over the lockdown period, the Nemesis migration of POI's household business from BGL has been completed without significant issues. This now represents a considerable opportunity for further growth.

20. We will update the POL ARC in the course of the meeting on any developments following the POI deep dive into Covid-19 related risks.

Appendices

Appendix A – Overview of POI Risk Management (Attached)

Reading Room:

- Report to the POI ARC on 14 May 2020: Analysis of the proximate Covid-19 risks and potential mitigants. Includes Appendix A, Scoring and Impact Table.
- Appendix B, Covid-19 Risk Management: Return to Work
- Appendix C, Customer Outcomes During the Covid-19 Crisis

POL00401577

Appendix A

How does POI approach the Management of Risk?

21. Our approach to risk management is set out within the POI Risk Management Policy which is approved annually by the Board (the last version being approved in September 2019). In common with most financial services business the policy notes that POI operates a three line of defence model. Risks are formally owned by first line Managers who are responsible for ensuring that these risks are effectively assessed and controlled.

22. The second line of defence provides on-going oversight and assurance that the first line is operating compliantly and effectively. The second line is undertaken by the POI Risk and Compliance team. The tools used to provide on-going assurance include risk based compliance monitoring in areas such as training and competence, financial crime and conduct risk as well as risk based thematic reviews. The second line of defence uses the information provided by 1st line together with regulatory developments and market information to provide a forward looking approach to risk and compliance issues.

23. Internal Audit provide a third line of defence by way of wholly independent review and oversight according to a pre-defined and approved annual audit plan.

24. In 2019 POI implemented the FCA regulatory requirements of the Senior Manager and Certification Regime (SMCR). Amongst other requirements including enhanced training and registration this regime required POI to designate granular management accountabilities within our business. This process has been linked to our wider risk management process so that accountabilities are linked to defined risks, and risks are in turn linked to controls. This link through accountabilities risks and controls has further strengthened our approach to effective risk oversight.

25. Overall risk appetites are set and agreed in conjunction with the POI Board. These provide clear statements to guide what levels of risk are acceptable within our business. Risks are identified and categorised throughout each business process and are scored on a defined 5 by 5 table which identifies impact and likelihood. A well-established risk system-Xactium is used to store risk and control information. Each control is assessed as either effective, partially effective or ineffective. The assessment is based on a variety of feedback loops used within the business which include MI, self-assessment of risks (carried out at least every six months) and second line review. Action plans are developed to address any areas where risks are considered as out of appetite by Management.

26. In addition to the Risk Policy, POI also operates a conduct framework which captures POI's approach to achieving good outcomes for customers. This ensures that POI continues to operate within its customer risk appetites and its regulatory risk appetite. The framework is focused around product design, pricing, sales quality, claims experience, feedback loops and POI's culture and strategy.

27. Oversight and challenge to these frameworks is provided at Management level via a formally established Risk and Compliance Committee, and at Board level via a formally established sub-committee of The Board- the Audit and Risk Committee. This Committee is chaired by a Non-Executive Director.

POL00401577

28. A risk dashboard is presented to the RCC and ARC which shows risks which are out of tolerance, key conduct concerns and the results of recent risk reviews. Actions arising from these Committees are formally tracked.

POL00401577

POST OFFICE LIMITED AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	Risk, Compliance and Audit Report	**Meeting Date:**	19th 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.

8

Confidential

POL00401577

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.

8

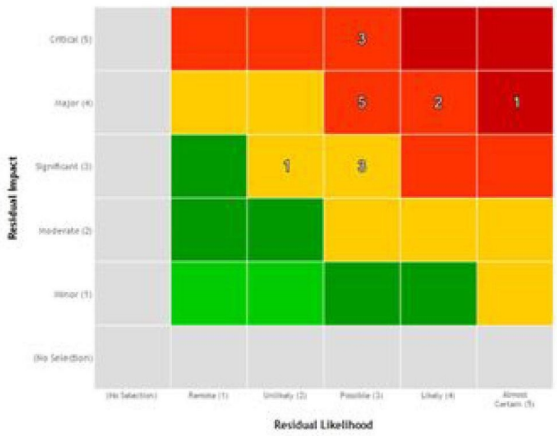


Figure 1: Post Office enterprise risks: April 2020

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

POL00401577

- **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.

POL00401577

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 if mitigations were not proactively identified or delivered. 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.

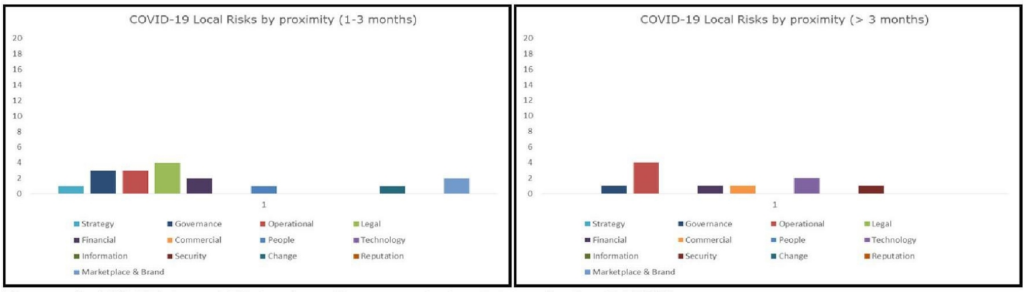


Figure 1: COVID Local Risks (medium- and short-term): April 2020

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

POL00401577

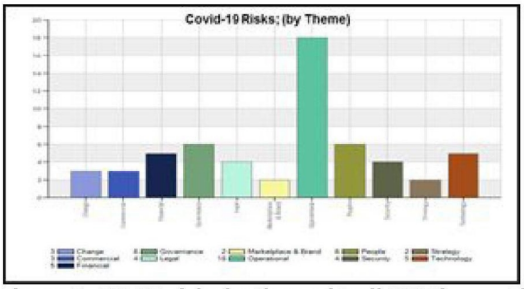


Figure 2: COVID risks by theme (April 2020)

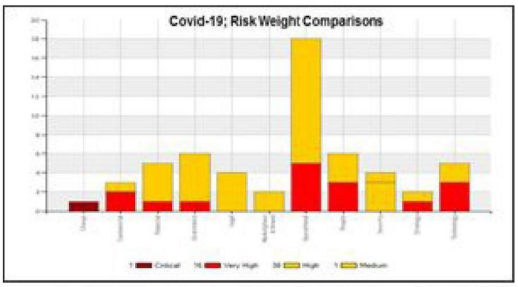


Figure 3: COVID risks by RAG distribution (April 2020)

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.

8

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 IRRELEVANT with full year spend equating to IRRELEVANT including GLO). The benefits achieved in March 2020 were IRRELEVANT with a full year total of IRRELEVANT 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:

POL00401577

- 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

8

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

Confidential

POL00401577

- 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 have worked with the DCMS to sign up to those commitments relevant to Post Office. This is in line with the rest of the Telecoms industry and will be announced by DCMS with a quotation from UK CEOs, including Nick Read. By working with our suppliers and careful positioning of our current product and policies with DCMS, we have delivered this at no cost to the Post office.

Vulnerable Customer Commitments

- Upgrade to Fibre for NHS clinicians – TalkTalk has agreed to fund the upgrades and Fujitsu Telecoms (FJT) has agreed to do the integration work pro bono. The volume here will be very low.
- Data Caps – we have a small number of legacy customers on capped data products, there is no variable charge from FJT on these lines and we do not charge customers for exceeding limits, therefore temporarily removing these caps comes at no incremental cost to Post Office.
- Late Payment and financial hardship – We have not made any changes to our dunnings process, but have highlighted our collaborative debt approach to DCMS (e.g., get well plans, no late payment fees etc.). We have extended the vulnerable customer policy to explicitly include vulnerability caused by Covid-19. The team continues to monitor debt workflows and although we do expect to see an increase due to wider economic impact from Covid-19 this subtle change will have minimal impact.
- Disconnections – Current policy does not disconnect customers for a minimum of 60 days after non-payment, we have therefore agreed not to disconnect customers in the short term as a result of Covid-19. This is a position we will continue to review. The exception here is customer fraud for which we will continue to disconnect.
- Calls Plans – we have made no changes to our calls plan offering, but have outlined to DCMS our fair and reasonable pricing and policies on our call plans (e.g., no minimum term, longer off peak etc.), which has met DCMS' criteria.

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.

POL00401577

- Phase 3 will deliver Post Office a compliant solution by enabling us to credit customers for any overcharge in the same billing month. We have now had confirmation from Fujitsu that it will implement a fully compliant solution by August 2020. We are updating the FCA with our progress and will then 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 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:

POL00401577

- 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 The solution for resolving the outstanding Cookies issue has been built and been deployed on the Post Office website.

31 As previously reported to and agreed by the Committee, this solution does not completely address the new consents guidance from the ICO but it does provide strong protection for customers and helping sustain commercial viability. This does position Post Office "in the pack".

8

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 asked a series of supplementary questions to which we responded on 30th April 2020.

34 Given the nature of this incident it was possible that Post Office would face regulatory sanction. However, in recognition of the immediate actions we have taken to rectify the process failings and the support package we will offer to those impacted, such as identity theft insurance and credit reference checking, the ICO has decided to take no further action. It has made some advisory comments, which we will look to implement as appropriate.

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

POL00401577

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. In order to meet the 2021 timeline Compliance, Legal and IT will work with the contract owners to address client concerns, 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.

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).

POL00401577

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. The situation is being kept under review and alternative ways to investigate will be sought if the current lockdown situation continues.

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).

- HMRC has agreed to a further suspension for May.

49 Additionally IRRELEVANT IRRELEVANT

50 In recognition of this and the financial challenge Post Office is facing as a result of the Covid-19 crisis, Compliance and Government Affairs have requested, through contacts in HMT, BEIS and HMRC that HMRC either cancels the annual registration fee for 2020/21 or that it allows Post Office to delay payment until it has been able to de-register these branches and has assessed the impact of Covid-19 on the remaining Travel Money branches. The business estimates that there may be a further two to three thousand branches that it may need to de-register in a post Covid-19 marketplace.

- HMRC has now advised that payment of the annual fee can be deferred until 1st December 2020. However, it is still intending to calculate the fee against the branches registered in June. This does not address our key financial challenge and we continue to lobby to have our request agreed. HMRC has advised that it is aware of the challenge we face and is discussing this at a senior level.

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 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.

POL00401577

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.
- We have assessed Post Office's provision of the Lottery as a low risk activity.
- 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.

8

Financial Services

Compliance Monitoring

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;

POL00401577

- 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 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

Confidential

POL00401577

70 For P12, overall mystery shopping performance has dropped to 46% (Inland and International mails being 40% and 73% compliant respectively). Whilst the Voice of the Customer data remains fairly consistently around 75%, the main reason for the poor mystery shopping results is that branches are failing to ask clarifying questions of the customer and put on the appropriate restricted label where required (following the Horizon prompts), leading to items being accepted incorrectly and non-compliant.

71 There are currently 9 different mystery shopping scenarios that IPSOS use in branch, which are representative of the volumes of items that are sent through the network. We have always performed better with the international scenarios as this is easier for colleagues and customers to understand (the items all go by air) and there is less confusion over the distinction between restricted and prohibited items. For domestic mails we have always struggled with the lithium battery/mobile phone restricted scenario.

- Until June 2019 this scenario was not used every month and we had no true meaningful comparison for year on year performance. This has now been changed, with the scenario being used every month as one of the domestic restricted scenarios to give a truer reflection of actual performance. This has resulted in slightly lower monthly scores for domestic items.
- In April 2020 we changed the scenario from a mobile phone with (but not connected to) a lithium battery, which with most modern smartphones is unlikely to occur, to a camera with (but not connected to) a lithium battery which we believe is a more likely combination to be sent.

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. Currently the project is at the planning stage.

Confidential

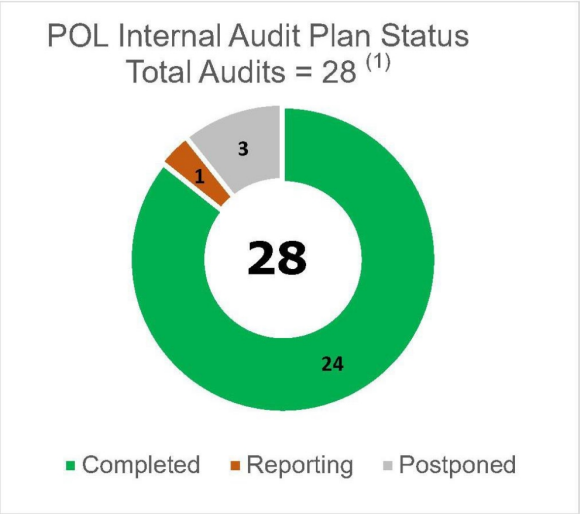
POL00401577

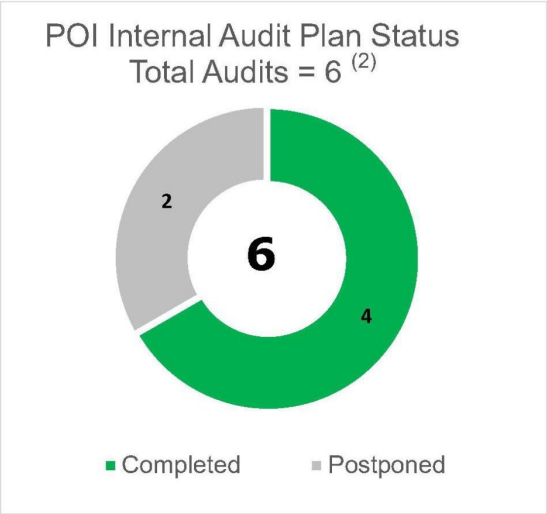
Internal Audit

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, including one report which was 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

8

Confidential

POL00401577

Internal Audit reviews completed

81 COVID-19 priorities have delayed audit fieldwork and clearance of audit reports during March and April. We have completed five reviews since the March ARC meeting, including one reports which was 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)	
5	FS Branch Sales (Final Draft)	

82 Our findings and observations from the four final reports are summarised below, with the full reports available in the reading room (appendices 11-14).

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."

8

Confidential

POL00401577

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

8

POL00401577

3. **Change Control Framework (Operating Effectiveness)** (Ref. 2019/20-24)	
 ***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 fully operational, 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."	

8

4. **Savings Products (Product Risk Review)** (Ref. 2019/20-26)	
 ***Sponsor:*** *Owen Woodley* Audit actions: P1 0 P2 1 P3 1 Total 2 *Appendix 14*	Processes and controls over Savings Products were found to be effective. The governance framework is clear and embedded, and provides a transparent forum in which decisions around product design, performance and compliance are reviewed, challenged and approved. Two findings have been raised (one P2 and one P3), which highlight the need to maintain standards around current activities. The P2 finding relates to the uncertainty over forecasting and concerns over the timing and nature of MI provided by BoI, principally stemming from a shift in commission calculation model brought about by the amended Financial Services Joint Venture Agreement. Management are well aware of these issues and are working with BoI to improve performance in these areas. Overall, this report is rated Satisfactory. We highlight that this rating extends only to those areas in scope and does not consider issues relating to the impact of Covid-19, nor any organisational design work currently underway.
Management Comment provided by Chrysanthy Pispinis – Post Office Money Director "We found the audit helpful, and welcome its conclusions and rating. We are very aware of the forecasting accuracy piece; the revised contract and new set of commercials that came into effect in October 2019 took some bedding in, exacerbated by a pressured mortgage market and emergency base rate cuts – all of which impacted our forecasts. We will continue working closely with BoI to ensure forecasts are as accurate as they can be."	

Confidential

POL00401577

Status of Audit Actions

83 Audit actions are generally being completed on time, however, we highlight that the changes to business priorities due to Covid-19 have caused delays in completion of some audit actions. We have been working with the action owners and GE sponsors to agree revised completion dates, where appropriate and with justifiable reasons. We will report as overdue any actions that are not completed by the revised dates.

84 The movement and ageing of audit actions are shown in the table below (status at 11 May 2020).

Audit Action Status (POL):	
Open actions at last ARC	64
Less: Actions closed in period	48
Add: New actions in period	38
Total open actions	**54**

Ageing:	
Open (not yet due) [N1]	54
Overdue (<60 days)	0
Overdue (>60 days)	0
Total open actions	**54**

[N1] Includes 14 actions for which revised dates have been agreed due to Covid-19.

85 Since the March ARC we have agreed revised dates for a total of 14 audit actions for reasons relating to Covid-19:

- Belfast Exit – 8 actions;
- IT Contract & Vendor Management – 3 actions;
- SGEI Validation – 3 actions.

8

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
Appendix 14: Internal Audit Report – Savings Products

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

Confidential

POL00401577

Post Office Limited
Year ended 29 March 2020

Audit and Risk Committee Report
Private and confidential
May 2020

pwc

POL00401577

Update to the Audit & Risk Committee

Scope and status

Overview and status

At the time of writing we are three weeks into the performance of our audit testing which is being carried out remotely in light of the current situation with COVID-19. Despite this we are making reasonable progress and although we are all having to adapt our working styles and do not have the benefit/ efficiency of being physically with the POL team in Chesterfield, we have not yet faced significant disruption and would like to thank all involved in the audit so far. The main impacts have been as follows:

- In anticipation of the "Lockdown" restrictions imposed by the Government on 24 March we brought forward our attendance at the year end physical cash counts at the Cash Centres to the weekend prior to the year end. Additional "roll-forward" procedures are therefore being undertaken to validate these cash balances at year-end;
- There are delays in receiving the forecasts which support POL's going concern assumption and asset impairment models, as management are updating these in light of the reforecasts required due to current situation; and
- Workings required to support the fact that POL has met the eligibility requirements to receive the Network Subsidy Payment ("NSP") are outstanding, specifically the calculations evidencing that the losses of underperforming branches are in excess of the IRRELEVANT NSP income received in FY20.

Excluding these areas we have made good progress in auditing agents remuneration, payroll, property, plant and equipment (excluding impairment), intangible assets (excluding impairment), and depreciation, amortisation and interest expenses. Our testing is less advanced over revenue, where our testing has been delayed due to changes in system reports which have made revenue sampling more complex than expected. The audit of receivables, payables and investment funding is currently proceeding as planned.

We are working with management to ensure we finalise our work in each of these areas (see the significant accounting and reporting matters for the areas we expect to be ongoing at that time) ahead of our clearance meeting with Group Finance on 8 June 2020. We will update the Committee on our conclusions at the ARC meeting on 16 June 2020.

Scope and risk assessment

Our assessment of risks has not changed since we issued our Audit Strategy Memorandum ("ASM") in November 2019, other than for those updates referred to at the Audit and Risk Committees in January and March 2020. All risk areas will remain under review as the impact of COVID-19 continues to evolve and we will discuss any further changes with the ARC as necessary.

Materiality

As detailed in our ASM in November 2019, our benchmark for overall materiality is consistent with prior year and is based on the Group's reported revenue for FY20. We have therefore applied an overall materiality of IRRELEVANT (FY19: IRRELEVANT) based on IRRELEVANT of the above measure and have used a performance materiality of IRRELEVANT (FY19: IRRELEVANT) to direct our testing. We originally communicated an overall materiality of IRRELEVANT in our ASM, which has reduced due to lower revenues in March 2020.

We have used a de minimis threshold for reporting to the Audit and Risk Committee any uncorrected misstatements in excess of IRRELEVANT (FY19: IRRELEVANT).

A summary of uncorrected misstatements, and our final materiality, taking into account any identified audit adjustments, will be included in our report to the Audit and Risk Committee in June 2020.

Significant accounting and reporting matters

We have not summarised in this document progress in relation to the audit of the significant risks relating to going concern, impairment of fixed assets and impairment of intangible assets, as these are all subject to further management review, not least given the impact of COVID-19 on budgets and forecasts for FY21 and beyond. We will provide an update to the Committee on 16 June 2020.

On the following page we have summarised our progress on the audit of elevated audit risks, including assumptions in the pension scheme liabilities, VAT accounting, capitalisation of intangible assets, and the impact of the first full year adoption of IFRS 16.

Presentation and disclosure matters

Postmasters' Group Litigation Order ("GLO")

There are many uncertainties in relation to the ultimate outcome of the Historic Claims Process which allows former postmasters who were not part of the GLO to make a claim. We will continue to monitor the progress of the claims and work with management to ensure that any provisions / disclosures made in the Annual Report reflect the latest position at the point of signing.

Classification and recognition of Trading Profit

The Group has again used a three column format in the income statement in order to disclose what it considers to be the underlying results of the business. The draft financial statements show a trading profit of IRRELEVANT. Total investment expenditure in the year of IRRELEVANT (FY19: IRRELEVANT) has been recognised in the financial statements, of which IRRELEVANT (FY19: IRRELEVANT) relates to network programmes, IRRELEVANT (FY19: IRRELEVANT) relates to severance, and IRRELEVANT FY19: IRRELEVANT) to business and IT transformation. We are currently testing the classification and disclosure of these amounts to ensure they meet both the definition of the Group's accounting policy and the FRC's guidelines in this area.

Other reporting matters

Management override of controls: Non-rebuttable significant risk as required by ISAs (UK). We have progressed our procedures in respect of this risk for part of the year and whilst we are still finalising our documentation, we currently have found no evidence of material fraud through management override of controls. Our work on the remaining periods is underway, and we will communicate our conclusion in June 2020.

Fraud in revenue recognition: Rebuttable significant risk as required by ISAs (UK). Our work is still ongoing in this area, and we will communicate our conclusion to the Committee in June 2020.

1

POL00401577

Update to the Audit and Risk Committee (continued)

Other elevated audit risks

Assumptions in the pension scheme liabilities:
The draft financial statements show that the IAS19 calculation of the Group's pensions liabilities remains in a surplus position. Pensions were identified as an elevated audit risk due to the judgements and estimates required when valuing the scheme as at 29 March 2020. We have held discussions with the Group's actuaries and received the actuarial report and expect to complete our work over the assumptions in line with the audit timetable. Our work is progressing well although we are in discussion with management regarding the sufficiency of the contractual evidence which supports the appropriateness of recognising 7% of the RMSEPP multi-employer schemes' assets and liabilities.

VAT accounting:
Due to the different revenue streams within the Post Office, there are a number of arrangements in relation to VAT. However as there is minimal judgement involved we have deemed this an elevated risk rather than significant. Our work is ongoing in this area and we will communicate our conclusion to the Committee in June 2020.

Capitalisation of intangible assets:
There is an elevated audit risk that the costs capitalised in the year of IRRELEVANT FY19 IRRELEVANT do not meet the definitions within the accounting standard and may have been inappropriately classified. We are finalising our documentation of our samples in this area, and will communicate our final conclusions in our June 2020 report.

IFRS 16 - first year full adoption:
The Group has adopted IFRS 16 from 1 April 2019 using the modified retrospective approach which is a simplified transition approach that requires you to calculate the lease liability from the date of transition (rather than from the start date of the lease). Due to the magnitude of the expected balances and the judgmental assumptions applied in relation to the implementation of IFRS 16, this has been deemed an elevated risk. In FY19 management disclosed the expected impact on adoption in line with IAS 8,estimating a range between IRRELEVANT and IRRELEVANT for the right-of-use assets and lease liabilities at the transition date. We have received the updated models and workings which calculate an opening lease liability of IRRELEVANT and an opening right of use asset balance of IRRELEVANT IRRELEVANT Work is ongoing in this area.

The right of use assets relating to "open" directly managed branches form part of the overall POL fixed asset impairment assessment, given that the POL network is considered to be one cash generating unit ("CGU"). Also IFRS 16 provides a practical expedient that lessees do not have to test right-of-use assets for impairment under IAS 36 at the date of initial application. Instead, a lessee may rely on its assessment of whether leases were onerous immediately before the date of initial application and adjust the right-of-use asset at the date of initial application by the amount of any onerous lease provision. Management have applied this practical expedient.

The right of use assets relating to vacant (ie non-trading) directly managed branches are considered as individual CGUs for impairment purposes.

We have discussed the approach to impairment and onerous lease provisioning with management and will communicate our conclusions in our report to the June 2020 Audit and Risk Committee.

POL00401577

IT General Controls - Summary of results

IT General Controls - *The following page summarises our conclusions in this area which were discussed with the Audit and Risk Committee in March 2020. We have now completed procedures to cover the full financial year and subject to the satisfactory resolution of the minor outstanding matter referred to below, there are no new matters to report or substantive changes in the conclusions previously discussed with the Committee.*

Scope of work
Our work over IT General Controls ("ITGCs") considers the underlying systems environment (applications, databases and operating systems) of key financial reporting applications. In accordance with our planned audit approach we assessed POL's Information Technology (IT) controls for the Horizon and Credence systems. We have performed testing for the the full financial year.

Preliminary conclusions
Throughout the year we have seen an improvement in the rigour and consistency applied to IT General Controls across the Horizon system. We have tested the Credence system for the first time and whilst issues have been found management has worked to address those throughout the audit period.

Across the financial year we have identified a total of 8 IT control deficiencies across the Horizon (3) (which includes 1 reported exception at Fujitsu) and Credence (5) systems. This includes one additional deficiency identified in the service organisation report received from Fujitsu as part of the top up work performed last month which had one low risk exception related to leavers access not being removed in a timely manner.

All 8 issues related to user access and security with three having a high impact, one medium and the remaining having low impact. The three high have been summarised to the right. The one medium deficiency related to the retention of documentation for the approvals for access requests for Credence not being retained. This was an issue for one sample out of four during interim testing for a user requesting read-only access. Testing was performed for Q4 with no exceptions noted.

Management has spent time remediating some of the issues identified at interim meaning that 3 (1 related to Horizon and 2 related to Credence) of the control deficiencies have been remediated as at the end of the financial year.

Due to the deficiencies identified, additional substantive audit procedures were performed to test for any inappropriate activity (e.g. inappropriate journal postings) in Horizon by users who have left the business or have enhanced and potentially inappropriate system access as well as activity testing over the global users within the Horizon system for the first part of the year prior to the super-user access control being remediated. The additional audit procedures concluded that the access issues did not give rise to any inappropriate activity,

Summary of key deficiencies
Horizon:
- Terminated application user access rights are not being removed on a timely basis (High)

Our testing focused on Post Office employees who left the company during the financial year and whether their Horizon accounts were disabled on their departure. Our testing was performed over 100% of the leavers population in the financial year. During interim testing we noted 2 POL employees who had left the company retained active Horizon accounts and at update testing we noted that 1 POL employee retained an active Horizon account. As these are POL employees within the Directly Managed Branches (DMB's) there is a risk that these accounts could have been accessed and invalid payments made. We performed additional procedures to confirm whether these user ids performed any activities in Horizon after the employee leaving date. Our work confirmed that no activities had been performed.
Through root cause analysis of the identified issues it was noted that there is an issue with the interface between SuccessFactors (HR) and the Smart ID system that manages access for Horizon. Through this investigation it was noted that 118 accounts that were historically disabled in SuccessFactors remained active in the Smart ID system, Management is currently working to validate whether these accounts have been used subsequent to the leavers termination date and identify a fix for the interface. We expect this control issue to be addressed as part of the enterprise wide IDAM project which should improve the leavers process.

- Super-user/ administrators and sensitive generic IDs are not monitored (High)

In response to our finding in the prior year (as communicated to the ARC in June/ July 2019) management have implemented a control to perform a bi-annual review to ensure the appropriateness of super users ('Global Users'). We have evidenced that this first operated in March 2020. During update testing this control was tested and no exception was noted. As the control was not in operation for the full year we performed additional substantive testing to evaluate whether the activities performed by users with Global User access were appropriate (we consider appropriate the activities performed by Branch Auditors, Training and Onboarding Team and authorised Agents). The additional audit work confirmed all activities performed with the accounts were appropriate. We have tested the newly introduced control.

Credence:
- Access rights to the application are periodically reviewed for appropriateness (High)

At interim it was noted that evidence was not retained to support the revoking of access that was identified during the review to no longer be appropriate (the medium deficiency referred to within the preliminary conclusions). Management addressed this area during the year however during our update testing it was noted that the review only covered users who had not logged in recently rather than also including leavers. We have performed additional substantive testing to validate that no leavers in the financial year inappropriately accessed the Credence system after being terminated.

Audit conclusion

On the basis of the control findings noted and the results of the additional substantive procedures performed, we will be able to proceed with our planned audit approach whereby we rely on the IT General Controls over the Credence and Horizon systems.

POL00401577

We have prepared this report solely for the use of Post Office Limited. This report forms part of the continuing dialogue between the Group and us and therefore it is not intended to include every matter, whether large or small, that has come to our attention. For this reason, this report should not be made available to third parties, and if any third party were to obtain a copy without prior written consent, we would not accept any responsibility for any reliance that they might place on it.

© 2020 PricewaterhouseCoopers LLP. All rights reserved. In this document, "PwC" refers to the UK member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.

POL00401577

POST OFFICE LIMITED
AUDIT, RISK AND COMPLIANCE COMMITTEE REPORT

Title:	FY19/20 financial close and Annual Report and Accounts	**Meeting Date:**	19 May 2020
Author:	Tom Lee - Financial Controller, Financial Accounting & Controls	**Sponsor:**	Alisdair Cameron - Group Chief Finance Officer

Input Sought: Noting & Discussion

The Committee is asked to **note** and **discuss** on the status of the FY19/20 close and proposed plans for the Annual Report and Accounts ("ARA") signing.

Executive Summary

The FY19/20 financial year has been substantially closed, with a few key items remaining open for subsequent adjustment. Post balance sheet event reviews are ongoing, with nothing significant noted to date beyond the open items known as at yearend. PwC are working through the yearend audit and will present a separate paper on status to the ARC.

Notable items to be concluded on, and hence yet to be reflected within the results, the ARA, and audited by PwC, include:

- Group Litigation Order ("GLO") and Starling activities – assessment to be made closer to the point of signing the ARA regarding the level of provisioning for certain activities, such as the Historical Shortfall Scheme, and associated disclosures to be made accordingly.
- Impairment reviews – the majority were performed prior to yearend however given the impact of Covid-19, revised reviews will be performed once amended forecasts and plans are confirmed.
- Going Concern – IRRELEVANT

IRRELEVANT

In light of the above, IRRELEVANT

IRRELEVANT

9

Confidential

POL00401577

Questions addressed

1. What is the status of the FY19/20 financial close?
2. What will be presented at the June ARC?
3. What are the plans and options for completion and signing of the ARA?

Report

FY19/20 Financial close

4. The financial year FY19/20 has been substantially closed, with draft performance reported to Board. The results show a draft trading profit of IRRELEVANT adjusted for bonus purposes to IRRELEVANT after removing accounting impacts, such as IFRS 15 and IFRS 16.

5. The results are currently in draft form due to the ongoing financial audit conducted by PwC and a number of post balance sheet event reviews being performed by the Post Office finance team.

6. As at time of writing, no significant items have come to light as a result of the post balance sheet event reviews which were not already known about prior to yearend (see point 7). These reviews will continue up to the date of signing the ARA, with adjustments made for any material events which come to light.

7. There are a number of significant items which must be concluded on prior to full closure of the financial year and correspondingly they may have an impact on signing the ARA. These include:

    a. GLO and Starling – A number of activities are underway following the settlement of the GLO during FY19/20, such as the Historical Shortfall Scheme. As these progress a view will be required as to what level of provisioning may be required, with adjustments made to the closing financial position and ARA accordingly. The timing of signing the ARA in relation to status of these activities will likely have a significant impact on the associated disclosures.

    b. Impairment review – Impairment can be split into a number of areas including individual assets, investments held and a review of each Cash Generating Unit ("CGU"). A number of reviews were performed pre yearend. However, given the impact of Covid-19 on the group's forecasts for FY20/21 and beyond, a decision has been made to re-perform a number of these reviews, principally for the significant projects, investments and CGU's, once revised forecasts have been agreed. The results of these reviews may require adjustment to the closing financial position and disclosure within the ARA.

    c. Going Concern – The group has a working capital facility of £950m from BEIS which is due to expire at the end of FY20/21. IRRELEVANT IRRELEVANT

9

Confidential

POL00401577

IRRELEVANT

8. PwC are currently undertaking their audit of the draft FY19/20 position and have prepared a report to present to ARC alongside this document. The report outlines the current audit status along with any initial findings. It should be noted that conclusion of the above items in point 7 covers many of the significant audit risk areas, and as such the conclusion on these will be critical to completion of the audit. Further details can be found in PwC's report to ARC.

June ARC

9. At the June ARC, Finance will present the following papers:

   a. ARA – the ARA will be presented in draft form for review and approval. This will have been through internal and external (PwC) reviews, but will be subject to amendments in respect of items noted in section 7. As such, the option to bring the ARA back to ARC at a later date may also be required.

   b. Briefing book – the briefing book contains commentary to support the financial position and performance presented within the ARA, including movement analysis and review of significant items.

   c. Accountable Person – a paper was presented at November ARC to provide an overview of the role of the Accountable Person. The June paper will provide an updated position in order to allow the CEO, as Accountable Person, to gain comfort over their ability to sign the ARA.

9

ARA Signing

10. As stated in point 7, there are a number of known outstanding items which need to be concluded prior to finalising the ARA. As a result there are several options available for signing of the ARA as presented below.

11. June/July 2020 signing. At this point, the GLO related activities will still be underway and therefore significant judgement will be required as to the potential impact, with associated provisions and disclosures made. The working capital facility IRRELEVANT IRRELEVANT albeit work is underway to try and achieve this. Furthermore the ongoing uncertainty surrounding medium to longer term market conditions due to Covid-19 will likely be an important consideration. Combining these factors means significant work will be required to evidence the group's ability to continue as a going concern at this point in time, with the IRRELEVANT PwC will also need to satisfy themselves as to the group's going concern decision. The perceived potential outcomes at this time are:

POL00401577

a

b

c

IRRELEVANT

12. Delayed signing. A three month filing extension has been granted to the group, allowing signing to occur anytime up to 31 March 2021. By delaying signing to a point up to this date it would allow more certainty to be achieved on many of the judgements presented in point 7, thus presenting a more factual / less judgemental ARA. However the level of certainty cannot be guaranteed due to unknown timings around key factors such as post GLO activities, plus the inherent unknown position of the market at a future point in time. Delayed signing also creates an additional administration burden with subsequent event reviews continuing for a prolonged period and PwC having to delay closure of the audit until such time.

13. The planned route as at time of writing is to aim for June / July signing, with the group being a going concern. This will depend heavily on the progress of discussions around funding facilities. If at this time the discussions are not progressed significantly enough to justify the going concern assumption, the preference is to delay signing until this has been achieved. At which point a view of the status of other pertinent items such as GLO, government funding cycle and market conditions will also be made and signing of ARA performed at a time that is deemed optimal.

Confidential

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	PCI-DSS Programme Update	**Meeting Date:**	19 May 2020
Author:	Jonathan E Hill (Compliance Director), Mark Baldock (Head of Risk), Johann Appel (Head of Internal Audit) & Joseph Moussalli (Programme Manager)	**Sponsor:**	Jeff Smyth (Group CIO)

Input Sought: Noting

The Committee 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 Ingenico final banking software deliverables are due in early February 2021 and this will allow branch rollout to commence 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 – The request to provide IRRELEVANT unding to enable completion of programme has been approved through PRB and IC. The business case will be presented to the Board in late May 2020.

10.1

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 payments and banking development reported on track.
- Key milestone: Ingencio has delivered the C3 banking specification.

POL00401577

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.

Risk

What are the key risks facing the business and what is being done to address these?

1. **Risk:** Risk of loss of confidence by our client base should a delay to the delivery 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.

2. **Risk:** Risk of the solution provider (Ingenico) encountering complexities while developing the banking part of the new solution as this is a new capability 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.

What are the emerging risks faced in the short and medium term and what is being done to address these?

3. The main short and medium term emerging risk relates to Covid-19 and the team is closely monitoring the situation and arranging teams to restart after lock-down clears.

How is the Risk Framework maturing?

4. The programme team identifies risks to the delivery of the PCI compliance. These are assessed for impact, probability and proximity. The risks are logged in Service Now and reviewed with the portfolio leads. The risks are scored in Service Now and owners and mitigation are identified.

   Risks and mitigations are reviewed at the following forums:
   - Project workstream level (IT workstream / TOM) - working group review
   - Programme risk review meeting
   - Programme Steering Committee
   - Portfolio lead review
   - RCC

   Specifically, in terms of risk maturity on the programme - the new payments solution from Ingenico that will form the core of the PCI compliance is in development and milestones for the overall programme have been refined.

POL00401577

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

Change is being managed through formal weekly supplier meetings with Fujitsu where progress against plan is reviewed and monitored as well as ongoing workstream review sessions with all suppliers.

This approach is enabling risks and issues to be identified early enabling quick decisions and escalations to be made as required.

Key operational risk and issues are being managed through this governance model and escalated where required to the Steering Committee meeting.

The key delivery challenges currently relate to the Coronavirus, as identified below.

5. **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.
   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.

6. **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.

Compliance

The PCI Programme is engaging with all parts of POL to deliver a PCI-compliant solution.

Telecoms

7. We have engaged with Operations and identified areas of the business that take payments over the phone. We are looking a solution with Verizon to use PCI Pal to take card payments over the phone securely.

Data Protection

8. We have engaged with the data protection team and there is one topic to be worked through. Ingenico has an Australian service team and data protection around this aspect is being confirmed.

POL00401577

Financial Crime

9. The Target Operating Model (TOM) remediation workstream is working closely with the Financial Crime team. Meetings have been held to look at working practices for investigating card fraud – this work is ongoing to find a suitable solution that is consistent with PCI.

Financial Services

10. The TOM workstream is also working with the Financial Services team to advise on adjusted IT systems and working practices that can be used with the new solution.

Internal Audit

Progress against Plan

11. Regular, monthly meetings have been held with Nettitude, POL's PCI Assessor. It is providing oversight and advice on the products, processes and development activities that the programme is performing.

Internal Audit Reviews in Progress and Planned

12. An internal audit report was issued on 6th January 2020 with the key outtakes and remedial areas identified. The latest PCI Prioritised Approach Document was created for review in late February and finalized across March / early April.

Status of Audit Actions

13. **Insufficient committed resources to support programme delivery (Priority 1)**
Impact: There is a risk that inadequate personnel and capabilities may result in an inability the achieve PCI compliance by the committed timelines
Action Taken: An internal programme manager has been recruited with knowledge transfer occurring across April and May to ensure a smooth transition. **Completed.**
14. **Incomplete assessment of PCI requirements (TOM workstream) (Priority 1)**
Impact: Non-compliant activities remain unmitigated following the completion of the programme exposing Post Office to fines and reputational damage
Action Taken: Business Requirements have been signed off and the TOM workstream has continued its review of all activities operating within the POL estate and the review of all products and processes is due to be completed by July 2020.
15. **Inability to fully demonstrate that the PCI guidelines were followed on the current proposed remediation (Priority 2)**
Impact: Inability to clearly demonstrate to governing bodies and key partners a comprehensive path towards achieving PCI compliance. Cost and remediation work needed to support further investigations including future QSA assessments.
Action Taken: IT requirements were signed off and agreed with suppliers. Process also put in place with internal Compliance and external QSA to review/approve each TOM remediation item.

POL00401577

16. **Business case approved in June 2019 has underlying weaknesses in its stated delivery timeline and benefits (Priority 2)**

Impact: i) There is an ongoing risk exposure of PCI non-compliance with wider impact in other processes, such as GDPR in instances of Data Protection Act breach.
ii) Programme benefits (cost avoidance and revenue protection) may be understated, limiting the ability to appropriately assess and provision for potential litigation and non-compliance costs including from potential data breaches.
Action Taken: An updated business case has been written that has incorporated and integrated supplier delivery plans and costs into the business case. This has progressed past the Project Review Board and Investment Committee and is due to be presented to the Board on 26th May.

17. **Assumptions within RAID log need additional evidence and change log not thoroughly documented (Priority 2)**

Impact: Ineffective delivery of the programme resulting in delays in achieving a compliant status or significant remediation with further PCI exposure.
Action Taken: All change requests are being progressed through the RTQ / Service Now change process.

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE

Title:	Cyber Security Strategy Update	**Meeting Date:**	19 May 2020
Author:	Tony Jowett, Chief Information Security Officer	**Sponsor:**	Jeff Smyth, Interim Group CIO

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 status and plans regarding the reduction of risk associated with Joiners, Movers and Leavers (JML)
- 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.

10.2

A stated in the previous paper all organisations need to manage people joining, moving roles internally and ultimately leaving the organisation to ensure the correct levels of IT access, payroll and building access are granted. Whilst COVID-19 has absorbed much of our focus and effort in the last 7 weeks there has been some good progress in this area.

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

POL00401577

Questions addressed

1. What is our current Cyber Security maturity vs. target and what are our plans for 2020/1?
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.

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).

Confidential

POL00401577

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.

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.

POL00401577

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.

25. We continue to focus on joiners, movers, and leavers (JML) – progress is described in the next Section.

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.

POL00401577

Report – JML

27. In the last paper we laid out or plans to reduce the risks associated with JML. Since then the need to secure the IT response to COVID-19 has taken much focus and attention, resulting in the Post Office being able to continue operations safely without its physical back office space being open.

28. Even with necessary attention being absorbed elsewhere there has been some progress on JML. Our overall JML plan is shared in Appendix 3 with the status of actions for Q1. Areas where we have made progress are shown below.

29. For ***Colleagues with standard access*** we gained approval for a project to address the integrity gaps in the current system but due to COVID-19 pressures we lost our original skilled resource to complete this work. We have now identified a replacement and the work has now started in May 2020 and is expected to complete by 31 July 2020.

30. For ***Colleagues with elevated & privileged access*** the annual PWC audit identified two low scored risks connected with the management of identity on our branch systems. The identity teams are reviewing the input from the audit team and will correct any process or control discrepancies.

31. For ***Third parties running own JML for POL outsourced systems*** – security management meetings continue with reporting the declared status of our providers

32. On our ***Underpinning technical infrastructure,*** we have performed a review and clean out of orphaned accounts in our directory systems to reduce the risk of unauthorised access.

33. We are developing a revamped JML plan in response to the new operating environment the Post Office is moving into. This will aim to standardise JML processes across all domains considering the requirements of a hybrid remote/office model and reinforce the roles of staff and line management in this.

Report – Protecting Ourselves on Social Media

34. 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.

35. 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.

POL00401577

36. 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.

37. 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.

38. 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.

Confidential

POL00401577

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.				

Confidential

POL00401577

	Red Team events planned for 2020 to further develop SOC

Appendix 2 – Communications from Results of Fake Phishing Attack

one update

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

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

10.2

Confidential

POL00401577

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 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

10.2

Confidential

POL00401577

Appendix 3 – JML Plan Status

Areas	Gaps	Plans
Colleagues with standard access	• There are some identified integrity issues where the key components can be out of step with each other as it is possible to make manual interventions in response to urgent security and HR events. • Several additional systems (Kaizala, Text Blast etc) require manual intervention to support JML activity.	• In Q1 2020 a project is being proposed (subject to approvals) that will address many of the integrity issues with the current automated system. – IN PROGRESS • In Q2 2020 a review of those systems that are not currently connected to MIM will be conducted with recommendations for closing the gaps. • In Q2 2020 Internal Audit are planning to conduct a follow up audit of JML
Colleagues with elevated & privileged access	• Post Office has several sensitive systems (including Credence, CFS) where a small number of Post Office staff under tight control of an administration team have access to make changes to users' access and their rights • The current processes for these are stringent and commensurate with the data under control.	• The annual Financial Audit conducted by PWC reviews and makes recommendations on access control to these systems. In Q1 2020 the results of the audit will be reviewed and actioned accordingly. - COMPLETED
Third parties with physical access to core locations	• There is the possibility that someone ceases to work for the Post Office account from a third party but that their access is still open, and their badge is still active. Closing this off requires the manual intervention of the sponsor currently.	• In Q1 2020 requirements for metrics and reporting will be produced that identify gaps in the overall process (including this area) and the size and scope of any issues in this area. NOT STARTED
Third parties running own JML for POL outsourced systems	• We are reliant on the honesty of the outsourcers to report JML stats accurately and appraise us of any issues – there is little in the way of a concerted audit programme at present. • The contracts are likely to be out of alignment with our revised Post Office security policy and industry good practice.	• In Q1 2020 develop an audit and/or audit log plan for JML with outsourcers NOT STARTED • In Q2 2020 perform a review of existing contracts and their JML-related content for currency and consistency with recommendations for changes
Underpinning technical infrastructure	• There are several technical components that are required to deliver JML • There are some perceived gaps in these areas including Active Directory • The move to cloud will also require changes and enhancements to these areas • JML metrics need to be established to inform areas for improvement	• Review the stability and integrity of our Active Directory system – this is a core component of JML. Target date Q3 2020. • Develop suitable metrics and reporting to identify improvement areas within JML – Q2 2020 • Review the opportunity to introduce further automated functionality including two-factor authentication to further improve JML – Q2 2020 • Convene a cross Post Office working group on JML – Q1 2020 NOT STARTED
Automation & Centralisation	• In line with industry best practice there should be a centralised Identity and Access Management team (rather than individuals being spread across several Post Office departments) with responsibility for managing identities and access rights of all individuals working with Post Office. • This team should also be supported by an automated system to increase accuracy and productivity	• The requirements for this capability and associated business case will be developed in Q2 2020

Confidential

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITEE REPORT

Title:	Progress Update on the Pilot Implementation of the Contract Management Framework	**Meeting Date:**	19 May 2020
Author:	Sherrill Taggart, Interim Legal Director	**Sponsor:**	Ben Foat, Group General Counsel

Input Sought: Noting & Decision

The Committee 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 Committee is asked to **approve** 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 Group Executive ("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 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.

11

Previous Governance Oversight

- Post Office Audit, Risk & Compliance Committee ("ARC") Meeting of 25 November 2019.
- Project Review Board of 14 January 2020.
- GE Tactical Meeting of 12 February 2020.
- Post Office RCC Meeting of 10 March 2020.
- Post Office ARC Meeting of 26 March 2020.
- Post Office RCC Meeting of 6 May 2020.

Confidential

POL00401577

Executive Summary

1. 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.
2. 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 75 Material Contracts and to have identified benefits of c£440,000[2].
3. This however leaves circa 70 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.
4. To complete the implementation for all Material Contracts (145 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.
5. Given the current commercial environment within which the Post Office is operating, the recommended approach is to complete the implementation for all 145 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

11

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	145	145
No. of Confirmed Latest Versions of Material Contracts	All (145)	96	145

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

POL00401577

Measurement	Original Target	Current Position	Forecast Position at Closure (19 May 2020)
No. of Material Contracts with Contract Managers	All (145)	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	64	75
No. of Material Contracts with Obligations Mapped	50	64	75
Rebates identified & Realised	Not Quantified	IRRELEVANT	
Other Value adds Identified	Not Quantified		
Spend vs approved	IRRELEVANT		

11

4. In addition to the numbers set out above, 28 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 **appendices 1 and 2** respectively.

5. The ARC 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.

6. The following options are available to the ARC:

[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 IRRELEVANT is the difference between providing external training or not. Other material savings which have been made against the original budget include IRRELEVANT in external legal advice, IRRELEVANT in programme resource costs, IRRELEVANT in licence fees and the quote from the external training providers was IRRELEVANT below the original provision.

POL00401577

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 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.	• C70 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 145 material contracts with	• We expect to be able to locate, upload onto Web 3.0, and	• The current run rate for the programme (excluding external	• Post Office would not have the complete picture of its	YES

11

POL00401577

Option	Timeframe to Complete	Cost Implications	Residual Risk	Recommended?
no further implementation or rollout thereafter	map the obligations for all 145 material contracts by 30 June 2020[5]. • For speed, the obligation mapping may however have to be done without the contract manager.	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.	contractual landscape, and be exposed to the risks described in previous papers to the ARC, 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 145 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

11

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

   • 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.

[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.

POL00401577

- 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.

POL00401577

Appendix 1 – Material Contracts Mapped

	Contract Name	Other Party
1	Horizon	Fujitsu
2	AEI Contract	Thales
3	EUC	Computacenter
4	Back Office IT Tower	Accenture
5	CDP Agreement	Accenture
6	Self-Service Kiosk	NCR Ltd
7	PED	Ingenico
8	Portfolio & Service Management	ServiceNow
9	Travel Insurance	Collinson Insurance Services Ltd
10	Travel Insurance	Ergo Travel Insurance Services Ltd
11	Royal London Life Contract	Royal London
12	Duck Creek Policy	Duck Creek
13	Technology Services	Accenture
14	Car, Van & Home Insurance	BISL
15	Home Insurance	Ageas
16	AllPay Bill payment	AllPay Ltd
17	UNUM Annual Group Income	UNUM
18	EDF Bill Payments	EDF
19	Money Transmission Services	MoneyGram Payment Systems Inc
20	Banking Framework	Various
21	Verizon Tower Contract	Verizon
22	BT Bill Payment Agreement	BT Telecommunications plc
23	Bank of Ireland : ATM	Bank of Ireland
24	Ingenico Paystation	Ingenico
25	WH Smith RAA	WH Smith High Street Ltd
26	Home Phone & Broadband	Fujitsu Services Ltd
27	Splash SaaS	Splash
28	FOCS	DVLA / CCS
29	AWIN Marketing Contract	AWIN
30	PowerNI Bill Payment Agreement	PowerNI
31	External Audit	PWC
32	3rd Party Data Audit	Grant Thornton
33	Money4Life - Pension	Zurich (soon to be Scottish Widows)
34	Interims and Contractors	Intelligent Resource
35	Office 365	Microsoft
36	NFSP Grant Framework Agreement	NFSP
37	Bank of Ireland: FSJVA	Bank of Ireland
38	POL's Outsourced Contact Centre (Home Insurance) (POMS)	Firstsource Solutions UK Ltd
39	POL's Outsourced Contact Centre (Travel, General Insurance and other Products) (POMS)	Telecom Services Centres Limited t/a Webhelp
40	Digidentity: Verification of ID	Digidentity
41	BUPA: Private Health Insurance	BUPA
42	Media Audit	Ebiquity Associates Ltd
43	Creative Agency	Ogilvy & Mather Group (Holdings) Ltd
44	Mails Distribution Agreement	Royal Mail
45	POCA	EntServ UK

POL00401577

46	Benefits Platform Provider x2 (one for POL and one for POMS)	Sodexo
47	DWP: POCA	DWP
48	ATM Agreement: POCA	JP Morgan
49	Digidentity: Verification of ID	Digidentity
50	Software Reseller	SCC
51	Mailwork Agreement	Royal Mail PLC (POL only)
52	Media Planning	Carat
53	Print Management	HH Associates Ltd
54	Master Franchise Agreement (Project Paddington)	WH Smith
55	Cabinet Office	DWP (Cabinet Office)
56	Gift Card Agreement	Blackhawk Network Europe Limited
57	Audit of Bank of England: Note Circulation Scheme	PWC
58	Audit of BEIS Loan	PWC
59	Audit of DVLA	PWC
60	Audit of Royal Mail: MDA	PWC
61	The National Lottery Retailer Agreement	Camelot UK Lotteries Ltd
62	Provision of Goods and Services relating to Safes and Secure Cash Storage	Insafe
63	Collective Engagement and Industrial Relations Framework	CWU
64	Collective Engagement Framework	Unite

Appendix 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	Santander
nPower	Quadrangle	Santander : Payout
Ingenico	Trinity McQueen	British Gas: Bill Payment
Scottish Power	Kantar	Mediazest
SSE Energy	ABA	McKinsey & Company Inc UK
Yorkshire Water	GFK	Royal Bank of Scotland
Capita Travel	Kouros	UKGI
Postmaster/Main/Local : Agency and Branch network	FRES: Foreign Currency Exchange	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
POMS : Distribution Agreement	WorldPay	
BEIS : Government funding provision of network	Bank of England (Note Circulation)	
BEIS : Entrustment Letter	1) Belfast Bunker = LCC Fuel 2) Birmingham = Certas Energy 3) Hemel = Watson Fuel	5) Portland Fuel Fuel Trading

11

POL00401577

	4) Newcastle = Certas Energy 5) Norwich = Watson Fuel	Company – Provide Fuel Hedging

Appendix 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.

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Law & Trends Report	**Meeting Date:**	19 May 2020
Author:	Sherrill Taggart (Interim Legal Director)	**Sponsor:**	Ben Foat (Group General Counsel)

Input Sought: Noting

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

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.

12

Strictly Confidential

POL00401577

Appendix 1

1. Law & Trends Report: New material updates

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
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 are now 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 2019 and therefore April 2020 is the first reporting cycle under SECR.	[redacted]		
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	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			

Strictly Confidential

POL00401577

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	actions of a former employee and exposed organisations to group claims where this had occurred.	the business of the employer and were not in an effort to deliberately harm the employer, as in the Morrisons Case.	[redacted]		
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 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.			
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	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			

Strictly Confidential

Post Office Limited - Audit Risk & Compliance Committee-19/05/20

POL00401577

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
	COVID-19 pandemic, and out of this introduces several employment changes. There has also been changes made to existing employment legislation.	Scheme launched on 20 April, and was due to run until the 30 June, but has since been extended until the end of October; 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; 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 reasonably practicable for someone to take some or all of their leave due to the effects of coronavirus, carry over of the 20	[redacted]		

POL00401577

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		statutory days' holiday will be allowed for up to 2 years; and d) Gender Pay Gap Reporting Postponed – At the end of March, The Government Equalities Office and the Human Rights Commission announced that enforcement of 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.	[redacted]		
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.			
		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			

Strictly Confidential

Post Office Limited - Audit Risk & Compliance Committee-19/05/20

POL00401577

Issue	Why it matters?	Latest Developments	Impact on Post Office	Action	RAG
		understanding in complying with regulations. Supervisory activity has been suspended, however the situation is being closely monitored.	[redacted]	[redacted]	[redacted]
		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.			

Strictly Confidential

POL00401577

POST OFFICE LIMITED
AUDIT, RISK & COMPLIANCE COMMITTEE REPORT

Title:	Supplier Contracts out of Governance	**Meeting Date:**	19 May 2020
Author:	Barbara Brannon, Procurement Director	**Sponsor:**	Alisdair Cameron, Group Chief Financial Officer

Input Sought: Noting

The Committee is asked to note the contents of the report.

Previous Governance Oversight

March 2020 - Quarterly Risk Report to the Risk and Compliance Committee ("RCC")

Executive Summary

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

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

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

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.

No new Risk Exceptions have been requested since those reported on and approved at POL Board on 8 April 2020. For completeness, these are reported against within.

13

STRICTLY CONFIDENTIAL

POL00401577

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. These were reported at a POL Board meeting on 8th April and there are no further incidents since:

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 IRRELEVANT in March to IRRELEVANT 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.

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

a) IRRELEVANT**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.

b) IRRELEVANT **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

13

POL00401577

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) IRRELEVANT **Brands/Rapp** – this expires in November 2020. A compliant route to market has become available via G-Cloud and a commercial process will be executed in the coming months.

d) IRRELEVANT **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 however, POL is currently reviewing its agreed sourcing plan against current business and operational constraints. A paper will go to GE and Board in due course if an alteration in commercial approach is proposed.

e) IRRELEVANT **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.

STRICTLY CONFIDENTIAL

POL00401577

Report

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

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

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

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

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

a) Low value, time constrained or highly sensitive/specialist engagements are not uncommon.

b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy and/or completion of large, and complex technical programmes of work to maintain or enhance services prior to a possible exit.

c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the 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

STRICTLY CONFIDENTIAL

POL00401577

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 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.

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.

STRICTLY CONFIDENTIAL

POL00401577

k) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
l) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues 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.

STRICTLY CONFIDENTIAL

POL00401577

Appendix A – All New Risk Exceptions

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)	IRRELEVANT		Medium	None	Medium threshold	IRRELEVANT
30/12/2019	Comms, R&I & PR	Corporate Affairs & Comms	Richard Taylor			Low	Pending	Medium threshold	
30/12/2019	Market Research	Corporate Affairs & Comms	Richard Taylor			Low	Pending	Medium threshold	
27/03/2020	IT Software	IT	Jeff Smyth (interim)			Low	Pending	PCR OJEU level	
29/03/2020	IT Software	IT	Jeff Smyth (interim)			Low	Pending	Medium threshold	
29/03/2020	IT Software	IT	Jeff Smyth (interim)			Low	Pending	Medium threshold	
29/03/2020	Media	Marketing & Brand	Emma Springham			Low	In flight	PCR OJEU level	
29/03/2020	Marketing	Marketing & Brand	Emma Springham			Low	None	PCR OJEU level	
29/03/2020	Banking Services	Operations & Supply Chain	Alisdair Cameron			Low	In flight	Lower threshold (PCR not applicable)	
01/04/2020	Occupational Health	HR	Alisdair Cameron			Low	In flight	PCR OJEU level	
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley			Low	In flight	Lower threshold (PCR not applicable)	
29/04/2020	Goods for Resale	Retail & Franchise	Owen Woodley			Low	In flight	PCR OJEU level	
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron			Low	None	Medium threshold	
30/04/2020	Management consultancy	IT	Jeff Smyth (interim)			Low	None	PCR OJEU level	
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron			High	In flight	PCR OJEU level	
01/05/2020	Staff Uniforms & PPE	Operations & Supply Chain	Alisdair Cameron			Low	In flight	PCR OJEU level	

STRICTLY CONFIDENTIAL