POL00401624

Post Office Risk and Compliance Committee Agenda

Date
4th May 2017

Start Time	Finish Time
13.00	16.00

Location
Room 1.19 Wakefield

Present	In Attendance		Apologies
Jane MacLeod(Chair) Paula Vennells Al Cameron Martin Kirke Alwen Lyons Rob Houghton Nick Kennett Kevin Gilliland	Johann Appel Richard Williams Amanda Radford Georgina Blair Deana Herley Jonathan Hill Jenny Ellwood	Russell Hancock Tim Armit Martin Hopcroft Sally Smith James Dingwall Sharon Gilkes	

	Agenda Item	Action Needed	For ARC	Purpose	Lead	Time
1.	**Welcome, introduction & conflicts of interest**			Members to declare any conflicts of interest	Chair	13.00 – 13.05 (5 minutes)
2.	**Minutes and action lists**	Approval		To approve the minutes of the meeting held on 9th March and update on the RCC Actions	Chair	
3.	**Risk Submission and Supporting Papers for ARA** **3.1** Top Risks & Risk Appetite **3.2** Executive Declarations **3.3** Risk Section of ARA	Discussion & approval	✓	To review the supporting risk papers prior to submission to ARC.	Richard Williams Deana Herley Chair	13.05 – 13.35 (30 minutes)
4.	**Risk update** **4.1** Supply Chain pilot of the Placemat **4.2** Business Continuity and Crisis Management update	Questions & noting	✓	To update the RCC on the placemat pilot, its objectives, goals and lessons learned. Also receive updates on approach to risk appetite and Business Continuity planning.	Deana Herley Tim Armit	13.35 – 13.55 (20 minutes)

POL00401624

Post Office Audit, Risk and Compliance Committee Agenda (cont.)

Agenda Item		Action Needed	For ARC	Purpose	Lead	Time
5.	**Key Operational Risks** **5.1** IT Controls **5.2** Financial Controls **5.3** Financial Crime **5.4** FS Conduct **5.5** Health and Safety **5.6** Transformation	Questions & Noting	✓	To note and discuss the top risks highlighted	Rob Houghton Amanda Radford Sally Smith Jonathan Hill Martin Hopcroft Jenny Ellwood	13.55 – 15.25 (90 minutes)
6.	**Internal Audit Report**	Questions & noting	✓	To note the Internal Audit Report	Johann Appel	15.25 – 15.40 (15 minutes)
7.	**Decision papers** **7.1** Modern Slavery	Approval	✓	To approve the statement for submission to ARC & Board, and note the implementation plan	Martin Kirke	15.40 – 15.50 (10 minutes)
8.	**Noting papers** **8.1** Horizon Scan **8.2** POMS RCC minutes **8.3** Whistleblowing Report **8.4** Identity Fraud Incident Report	Noting	✓		Chair Nick Kennett Chair Nick Kennett	15.50 – 15.50 (10 minutes)
9.	**Any Other Business**					
	CLOSE					16.00

POL00401624

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC Mar 2017**
Date: 09 March 2017	**Venue: Boardroom, Finsbury Dials**	**Time: 13:00 – 16:00**
Members:		
Jane MacLeod (JM)	Group Legal, Risk & Governance Director	Chair
Al Cameron (AC)	Chief Finance & Operations Officer	Member
Alwen Lyons (AL)	Company Secretary	Member
Kevin Gilliland (KG)	Chief Executive - Retail	Member
Martin Kirke (MK)	HR Director	Member
Paula Vennells (PV)	Group Chief Executive	Member
Rob Houghton (RH)	Group Chief Information Officer	Member
Attendees:		
Richard Williams (RW)	Senior Manager Risk	Report (Item 7.1)
Johann Appell (JA)	Senior Manager Audit	Report (Item 5)
Adnan Killedar (AK)	Risk Business Partner	Secretariat
Jonathan Hill (JH)	Head of Risk, Banking Regulation and Strategy	On behalf of Chief Executive – Financial Services and Telecoms
Jenny Ellwood (JE)	Head of Transformation Risk and Assurance	Report (Paper 3.5)
Martin Hopcroft (MH)	Head of Health and Safety	Report (Item 3.4)
Sally Smith (SS)	Head of Financial Crime	Report (Paper 3.6)
James Dingwall (JD)	Interim MLRO	Report (Papers 3.4 and 3.6)
Angela Van-Den-Bogerd (AVB)	People & Change Director	Report (Paper 3.5)
Tom Wechsler (TW)	Government & Payment Services Director	On behalf of Chief Executive – Retail
Sharon Gilkes (SG)	Business Performance ad IT Transformation Director	Report (Paper 3.2)
Deana Herley (DH)	Senior Manager Assurance	Report (Paper 6)
Apologies:		
Nick Kennett (NK)	Chief Executive – Financial Services and Telecoms	
Kevin Gilliland	Chief Executive – Retail	
The meeting began at 13.00		
Agenda Item 1, Welcome and introduction		
The Chair declared the committee quorate and opened the meeting.		

POL00401624

Agenda Item 2, RCC minutes and actions

The Committee agreed the minutes of the previous meeting and reviewed the open actions.

AP 1765 (Tax Governance) – AC stated that this will be included in the annual Treasury report and will be presented to the RCC.

AP1758 (Risk Appetite Workshops) – The Chair reported that the workshop will be held for GE members on 13 March 2017. The workshop will be moderated by Deloitte.

AP1748 (Fraud Reporting) – This will be covered as a separate agenda item (3.6). AC asked that a summary from past reported incidents should be included in the report. Revised report should be presented to the May RCC.

AP1742 (Vulnerable Customers) – The Chair stated that this will be covered under agenda item (4.1).

Agenda Item 3.1, Management of key operational controls

3.1 Financial controls

AC introduced the Financial Controls paper. AC stated that the Self-Assessment has been completed and the process is working well. PwC have carried out a sample based review. The PwC review has not flagged anything major, however, there are some individual pieces of learning. AC stated that the profile against Fixed Assets has changed. Barbara Brannon is carrying out a review of Purchase to Pay including POLSAP aging of items and review of accounts which will identify financial risks in this area. AC stated that this year focus was on financial controls. For next year, it is planned to enhance the scope to also cover operational controls.

3.2 IT controls

SG joined the meeting. SG introduced the IT controls update paper and provided an overview to the RCC. JM enquired about the project schedule, when it is expected to be completed and the benefits from the project. RH replied that the project is currently at the stage of process review and will highlight weaknesses / shortcomings in the existing process and suggest mitigations in line with the CoBIT framework. SG added that currently KPMG have identified eleven areas within CoBIT which will be reviewed as part of the project. Currently, three areas are being reviewed namely, Incident management, Problem management and Change management. The review will identify "owners" of the process areas and controls, identify gaps, remediation and will also identify contractual position and any gaps in them with respect to the process and controls.

RH added that once the review is completed, a clearer picture will emerge of gap in contracts. The decision can then be taken on how to address the gaps and the decision will be guided by our risk appetite. This will also help set PO standards for future procurements / outsourcing. AL requested update can be provided for the ARC (**AP1769**).

PV joined the meeting at 1:20pm.

3.3 Financial services conduct risk

JH introduced the paper on FS conduct risk. JH updated the RCC on the Conduct action plan which the FS & Telecoms team is implementing with the Retail team. JH informed that the plan is approaching its end as the actions are completing and will soon move into business as usual activities. JH stated that the key outstanding action relates to agreeing responsnibilities with the Retail team under the new organisational structure. JM reminded that an ARC update is due on conduct risk. AC suggested that the ARC update include:

- Difficult trends
- Overdue actions
- Status of red/amber actions including actions that have turned red/amber
- Any matters for the attention of ARC

POL00401624

PV enquired about the mystery shopper related point regarding mortgages. JH stated that this has been an area of focus and work is on-going with BoI and the mortgage team to address findings and that the required standards are met. JM asked if the Retail team has the capacity and capability to support the new structure.

RH enquired about if the FCA Senior Managers Regime affect Post Office. JH replied that it is contained within POMS and does not currently cover Appointed Representatives. JH also stated that PO is working very closely with BoI and POMS to understand how it can provide support to them with respect to their requirements under SMR.

MK enquired if PO responsibilities and/or accountabilities have been documented. JM replied that work was started across PO to document GE responsibilities and accountabilities. A draft was produced, but since, PO has undergone an organisational change and therefore the draft will need to be updated. The draft covered GE accountabilities. JM stated that she will consider how the current document can be updated keeping in view the new structure (**AP1770**).

3.4 Health and safety

MH introduced the paper on Health and Safety. MH presented the highlights of the paper, stating that PO has an excellent safety record. Focus is on emerging risks as a result of the changed organisational structure. A lot of work has been carried out by the Property team to reduce the risk which is now low.

JM enquired as to how we have communicated the changes in regulation regarding use of mobile phones while driving. MH stated that communications have gone out to all staff and another round of comms is planned. Also, a training programme is being developed which will include video. PV enquired if loss of productive time has been assessed as a result of the changes and if this has been factored into the objectives of the staff. AVB confirmed that this has been done for the fleet drivers. Other staff have also been made aware of the regulations and loss of productivity has been considered.

3.5 Transformation risk

JE introduced the Transformation Risk paper. JE provided the overview to the RCC stating that the risks have reduced and are still within the expected "themes". JE stated that work is on-going to have a single integrated plan for the Change Programme. The Committee discussed the Transformation Risk paper, noting that this was a good paper which demonstrated how risks were being managed and provided a commentary on the significance of each risk.

3.6 Financial crime

SS introduced the Financial Crime Annual Review paper. SS informed the RCC that HMRC have completed their audit and a meeting has been scheduled for 22 March to share the findings of the audit. SS stated that the focus would be on how to proceed from where we are and we will be assessing what needs to be done which meets HMRCs requirements. SS stated that she will need an extra resource to implement required improvements. JM stated One of the main findings of the HMRC audit is monitoring of transactions. Currently, Horizon does not have this capability which will need to be built. The RCC agreed that an assessment of the scope of work will be done and resource requirements can be discussed based on the assessment.

Agenda Item 4, Updates

4.1 Vulnerable Customer Policy (draft)

JH introduced the paper and stated that this is a difficult area given Post Office's diverse customer base and products. Specific regulations and requirements are easy to identify and include but there are more generic requirements which are open to interpretation and therefore it is difficult to

POL00401624

understand their requirements. The Committee discussed the policy and noted that staff and colleagues need to identify vulnerable customers across everything we do. JM stated that the policy could provide guidance across five key areas which need to be considered. The business units can then have the flexibility to develop their own processes. The RCC agreed that the draft will be updated based on discussions and that MK will review the policy before it is presented to the RCC **(AP 1771).**

4.2 Review of Code of Conduct Policy

MK introduced the paper. Steps to implement include development of training material. This fits well with the work being done on Employee Value Programme and the focus is on encouraging and enhancing positive behaviours. JM stated that there is no central induction pack for joiners. MK stated that there is a pack, but it is possible that it is not being distributed in all cases. AC requested that training for vulnerable customers and business code should be merged into a single course.

4.3 Review of Conflict of Interest Policy

AL introduced the paper on Conflicts of Interest policy. AL suggested that going forward, all Directors should declare if they have any conflicts of interest. JM agreed and stated that this should be part of the agenda of meetings and the Chair should see confirmation from participants whether there were any new or relevant conflicts. This also needs to include all GE direct reports. (**AP 1772**)

Agenda Item 5, Internal Audit Update

JA introduced the Internal Audit update paper. JA gave the Committee an update on the progress of the annual Internal Audit plan. No new reports were issued / finalised since the last RCC. JA stated that there is only one overdue action from previous audits. JM informed the RCC that the process of finalising an audit report includes clearance from the GE sponsor and other GE member(s) (if applicable). JA stated that draft report on the review of Identity Management will be issued this week which is a critical report.

JA stated that there have been a couple of changes to the plan. Review of IT Operations and Governance has been delayed keeping in view the KPMG review on IT controls framework. IA is instead providing assurance on the IT controls framework project. IT Third Party management review overlaps with the Transformation Third Party review and these reviews have been merged.

JA presented the 2017-18 Internal Audit annual plan. It includes 16 BAU and 13 Change audits. The RCC discussed the plan and made suggestions to do more detailed review of the Network Development Programme and Back Office Tower Transformation Programme. It was agreed that the plan would be reviewed and updated.

The RCC approved that the revised plan can be presented to the May ARC meeting. PV thanked JA on the work carried out by him and his team in 2016-17.

Agenda Item 6, Executive Declaration 2016-17

DH introduced the paper. DH reminded the RCC that Executives Declarations are sought twice a year, in March and September. The March process will start with the pack being issued in the coming week. The deadline for returns is 3 April 2017. GE members and their direct reports are required to disclose material events. MK enquired if these include any legal actions. JM stated that list of legal actions faced by PO are maintained by the Legal team and should be referenced in the declaration.

Agenda Item 7, Risk update

POL00401624

7.1 Risk incidents and exceptions

RW introduced the paper. RW stated that there has been a significant decrease in the number of incidents reported and requested the GE members to re-invigorate the process. The lower reporting levels could be due to the change in the organisational structure. RW also noted that the IT incidents have reduced. AC stated that his team is doing a review of procurements and there may be exceptions resulting from this review.

7.2 Business Continuity Planning

JM introduced the paper and stated that Tim Armit, the Business Continuity Manager will be providing an update in the next meeting.

Agenda Item 8, Noting Papers

The Committee noted the following papers

8.1 RCC effectiveness review against ToR

8.2 Brexit update

JM stated that Brexit risks are being monitored closely. Reports are being prepared, these are still early days and things may change as negotiations to exit start.

8.3 Horizon Scanning

JM introduced the paper and stated that the purpose of the paper was to identify what new risks may emerge in the future. JM stated that a Corporate Affairs Steering Group is being established which will also review horizon risks. PV enquired how PO compared to other companies with regard to para number 2 (page 2). AC stated that we have faced some problems which relate to the suppliers own internal processes. Barbara Brannon is working on this and her review will identify any improvements that may be required.

8.4 POMS RCC Minutes

The Committee noted the minutes of the December 2016 and January 2017 POMS RCC meetings.

Agenda Item 11, Any other Business

Nothing raised.

The meeting closed at 16.05

Next Meeting – 04 May 2017, Room 1.19 Wakefield 13.00 – 16.00

POL00401624

POL Risk and Compliance Committee
Action List

Status Report as at: 28/04/2017

Meeting Date	AP ref	ACTION	Action Owner	Due Date	STATUS	Open/ Closed
09/03/2017	1773	**RCC Terms of Reference** - to be reviewed and updated based on changes in PO structure	Jane MacLeod	20/07/2017		Open
09/03/2017	1772	**Conflict of Interest -** to be confirmed for RCC meetings by forming part of the agenda.	Alwen Lyons	05/05/2017	Included in item 1 Welcome, Introductions & Conflict of Interests in May 2017 RCC meeting	Open
09/03/2017	1771	**Vulnerable customers** - policy to be reviewed and updated based on RCC feedback. Martin Kirke to review draft policy.	Jonathan Hill/ Martin Kirke	20/07/2017		Open
09/03/2017	1770	**GE accountabilities map** - to be refreshed / updated based on the new structure.	Jane MacLeod	tbc		Open
09/03/2017	1769	**IT controls review** - update paper to be presented to to the ARC.	Rob Houghton	21/03/2017	Submitted to March ARC.	Closed
09/03/2017	1768	**Fraud reporting** - report to be updated to include past incidents. Present report at each RCC meeting	Sally Smith	tbc		Open
09/03/2017	1767	**Tax governance** - to be included in the annual Treasury report to the RCC/ARC	tbc	tbc		Open
10/01/2017	1766	**Risk reporting format trial**- Trial new reporting format in Supply Chain and provide update to RCC and ARC	Jane MacLeod/ Russell Hancock	05/05/2017	Included in item 4 Risk Update in May 2017 RCC pack	Open

POL00401624

3.1) Top Risks and Appetite

Author: Richard Williams Sponsor: Jane MacLeod Meeting date: 4 May 2017

Executive Summary

Context

The purpose of this paper is to provide an update on the profile of our Top Risks and Risk Appetite for reporting to the May ARC and to drive our risk governance disclosures in the Annual Report & Accounts, including disclosure of our "Principal Risks".

Questions this paper addresses

- The attached chart shows:
    a. The main risk categories consistent with those set out in the placemat.
    b. A comparison of red rated risks as at May 17, compared to the assessment undertaken in January 2017 (where red means a rating greater than 3:4 / 4:3).
    c. The applicable / most relevant risk appetite statement as set out in the Board approved risk appetite (Jan 2015).
    d. Any relevant references that help define the risk appetite.

- Risk Appetite and Risk Score are not related. In some instances we have key risks with no corresponding appetite statement and instances of appetite with no corresponding risks. How do we show linkage?

Conclusion

1. At the date of writing we have not yet had feedback from all GE members, although further meetings are scheduled ahead of the RCC. Any updates can then be discussed verbally at the meeting.

Input Sought

2. The Committee is asked to consider the proposed changes, as highlighted in blue, to our top risks for the disclosure and the risk appetite, including the impact of recent risk incidents, and suggest any further changes.

POL00401624

POL Key Risks and Appetite as at 12/04/17

			SECTION A: Group Risk Profile - May 17 (Red Scored Risks only)							SECTION B: Board Risk Appetite - (2015)							
	Principal Risk	GE Risk Owner	Risk Description	Score Jan-17	Score May-17	Position Jan-17	Position May-17	Key	#	Risk Appetite Statements (KEY: 1. Averse, 2. Neutral, 3. Tolerant, 4. Seeking)	Appetite 1	2	3	4	Principles of Risk Intolerance	Principles of Risk Tolerance
OPERATIONAL	Data Privacy & Records Mgt	Jane MacLeod							1	**Averse** risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences.	■					
	Outsourcing Governance	Alisdair Cameron	**Third Party Relationship Management** Fail to select, contract, measure, monitor and exit key in-source or out-source relationships/ contracts successfully and/ or unintentional breach of contractual terms by PO	4 - 4	4 - 4	3	4	Merged								
	Health & Safety	Alisdair Cameron							2	**Averse** risk appetite associated to the health, safety and wellbeing of POL customers and colleagues in everything we do. This is paramount to every aspect of POL operation. This includes; loss of life, serious injury and non-compliance to regulation and policy	■					
	BCP	Jane MacLeod							3	**Averse** risk appetite for inefficient or ineffective or prolonged failure of, governance and control processes, critical financial reporting processes, critical supply chain and business continuity processes.	■					
TECHNOLOGY	Financial Reporting and Control Failures	Rob Houghton	**IT Delivery Capability** Unable to deliver in line with our Transformation cost, benefit and delivery plans due to lack of strength in POL technical leadership capability, lack of continuity of key people in key roles, and/ or IT Change Programmes designed and configured around high risk single event implementations. Resulting in change either not being delivered at all or taking longer, costing more, delivering less with eroded benefits	4 - 4	4 - 4	6	6	Merged	5	**Averse** risk appetite for inefficient or ineffective processes that result in: lost time, duplicated effort, and increased risk of financial loss or errors in any part of its business or core processes	■					
									4	**Neutral** appetite for operational IT services		■				
	Cyber Threat	Rob Houghton	**Cyber Threat / IT Security** We have critical IT Security exposures highlighted by a third party (Deloittes) review across our security infrastructure. These relate to firewalls, pen testing and out of date infrastructure. We have mobilised a Security Transformation programme to mitigate this risk.	3-4	3-3	New in May	16	Merged	6	Averse appetite for data loss/leakage that can lead to customer, commercial or reputational damage	■					
	Info Security	Jane MacLeod	**Information Security / Data Protection Breach** Fail to adequately deploy and effectively manage data protection policies, standards and controls within the business and our partners/ suppliers, results in a breach of company data (colleague/ customer)	3 - 4	3 - 3	14	14	Merged	7	**Averse** appetite for data loss/leakage that can lead to customer, commercial or reputational damage	■					
	Dependancy on third parties	Rob Houghton	**IT Availability/ Ability to Trade** There are a number of our 3rd party suppliers which are supporting critical components in our IT Estate. The components have either reached the end of life or there is no back-up capability and could cause significant impact to the business if it fails. This risk is heightened against some of the Fujitsu infrastructure components due to the recent contract extension that only supports the restoration of service to some out of support components by "best endeavours". Work is underway to remediate where possible until platforms are modernised.	4 - 4	5 - 4	4	1	Merged	8	**Averse** appetite for inaccurate and unreliable processing of data.	■				1. An acceptance of Horizon failing – not currently within power to stop	
LEGAL & REGULATORY	Financial Crime & Fraud	Jane MacLeod							9	**Averse** risk appetite for financial crime to occur within any part of the organisation	■					
	Conduct (inc compliance,TCF, reputation,product)	Nick Kennett Kevin Gilliland	**FS Regulatory Supervision** FS products are designed and distributed in a non compliant way, T&C oversight is inadequate, regulatory failure as a result of inadequate risk management, guidance or support .	3 - 4	3 - 4	13	13		10	**Neutral** appetite for risk taking which would have a detrimental impact on vulnerable customers. Post Office will take a balanced view, reflecting commercial implications of introducing safeguards and controls to protect vulnerable customers and the needs of those customers.		■			1. Fines to do with non-compliance	1. Risk around customer service – however, looking to reduce risk
									11	**Tolerant** risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality			■			
									12	**Averse** risk appetite for not complying with law and regulations or deviation from business' conduct standards	■					
	Legal (inc, litigation, governance)	Jane MacLeod							13	**Averse** risk appetite for litigation in relation to high profile cases / issues	■					
									14	**Averse** risk appetite for ligation in relation to Financial Services matters	■					
FINANCIAL	EBITDAS Growth, inc Scorecard	Alisdair Cameron							15	**Tolerant** to risk-taking which will grow sustainable EBITDAS over time			■			
	Financial Resources / Cash		(NB> Financial controls risk currently classified as No 23)	2 - 4	2 - 4	23	24		16	**Averse** risk appetite for not having sufficient financial resources to ensure the continuity and sustainability of the company. This especially relates to ensuring that sufficient funding is always available	■					
									17	**Averse** risk appetite for disruption to any credit facility	■					
									18	**Seeking** risk appetite for reducing dependence on subsidies over time.				■		
	Commercially Sustainable (subsidy dependence)		**Government Funding and Headroom** Funding beyond 2017/18 is insufficient to support the investment and transformation programme and we breach our headroom requirements	5 - 3	5 - 3	1	2		19	**Tolerant** risk appetite to lose the engagement of any key stakeholder in the process and for staying the course in face of opposition if in the wider interests of the business and its commercial priorities			■			
									20	**Tolerant** risk appetite in taking forward its strategy in the corporate affairs environment- as it is recognised that there will inevitably be opposition and adverse comment – but if POL presents a clear, cogent, confident case it can create the right environment for change			■			
CHANGE	BAU	Alisdair Cameron	**Change Portfolio Delivery - Complexity** The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity to manage, which if not managed well could significantly impact our execution plan	4 - 4	4 - 4	5	5									
	Transformation		**Transformation Resourcing - Payroll Legislation** HMRC are making legislative changes which are effective from April 17, which could cause significant impact to Transformation's current resource model and threaten our ability to deliver Transformation Phase 2. Impacts include increase in costs, reduction in number and quality of contractor resource pool	3 - 5	3 - 5	7	7		21	**Tolerant** risk appetite for customer dissatisfaction caused by transformation, innovation and customer selection/profitability decisions.			■			
	Competitiveness	Kevin Gilliland	**Market Developments/ Competition (Retail: Mails & Govt Services)** Unable to respond quickly enough to new entrants with different strategies/ business models, current competitors with new products/ technologies, who take market share and/ or profitability	4 - 4	4 - 4	2	2		22	**Tolerant** risk attitude to pricing to drive revenue growth, but not to the point at which it becomes non profitable (Retail, FS&T)			■			
		Nick Kennett	**Market Developments/ Competition (Financial Services & Telecoms)** Unable to respond quickly enough to new entrants with different strategies/ business models, current competitors with new products/ technologies, who take market share and/ or profitability - includes BoI is not aligned (strategically or financially) to assist POL's growth plans	4 - 3	4 - 3	12	12		23	**Neutral** risk attitude in government services and telephony market where we will price competitively to retain market share (Retail, FS&T)		■				
									24	**Seeking** risk attitude in financial services to gain profitable revenue and market share.				■		

POL00401624

STRATEGY	Market (trust, brand, social purpose)	Kevin Gilliland Alisdair Cameron	**Network Proposition** Unable to retain and or/find sufficient new retail partners because of the complexity and controls of the current proposition and value to the retailer, which leads to a decline in network numbers below 11,500	4 - 3	4 - 3	8	8	A	25	**Averse** appetite for risk taking which would alienate or lose significant groups of profitable customers	■				1. To core products not being made available through all channels 2. To there being no branch in a particular location – a bad partner is better than no partner – very few partners are an 'absolute no'	1. To reducing central control to allow empowered front-line decision making 2. To the "Daily Mail Test" – the business can accept risk where decisions can be defended (e.g. transparent product pricing – Telco, special delivery) 3. To sustainability – prepared to chose lower quality partner in rural areas 4. To Non-core products being digital only
									26	**Averse** risk attitude when it comes to diversifying Post Office's product portfolio or for business initiatives that may have adverse reputational or brand impact.	■					
		Kevin Gilliland	**Royal Mail Alignment** Misalignment of objectives and unsuccessful renegotiation of MDA or renegotiation on disadvantageous terms	4 - 3	3 - 3	11	11	P A	27	**Seeking** risk attitude in the mails market where we will take on competitors in markets and consider reduced margin to defend market share				■		
	Customer Relevance (access, ability to trade)	Nick Kennett Kevin Gilliland Martin Edwards	**Customer Experience** Our customer experience, propositions and channel strategy fail to deliver what customers want	4 - 3	4 - 3	10	10	A	28	**Averse** appetite for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy	■				1. non-scalable products 2. non-core bank partners (e.g. credit unions) 3. unsustainable products 4. taking risk across all customer groups	1. a new core banking framework partner 2. accept lower quality and greater product complexity 3. complaint resolution on an individual basis
			Digital Competency Lack of digital competency to spot and implement quickly enough (e.g. new products, customer journey, back office)	3 - 4	3 - 4	15	15	A	29	**Neutral** risk appetite for dissatisfaction related to BAU services recognising that in a complex business there will be a level of dissatisfaction as part of the normal course of business of achieving our commercial objectives.		■				1. provide at all these branches, mails, basic cash and banking facilities, pay out services and bill payment facilities;
PEOPLE	Staff Resourcing	Martin Kirke							30	**Neutral** risk appetite for Misalignment of people capability and capacity of staff		■				
									31	**Neutral** risk appetite for Insufficient people capacity to enable PO to effectively deliver core services to customers.		■				
	Staff Engagement		**People Capability** There is no clear prioritisation of capabilities required to deliver the business strategy, particularly during current reorganisation	4 - 3	4 - 3	9	9	P A	32	**Neutral** risk appetite for Inadequate assessment of the necessary talent and capabilities identified in order to build the learning and development plan and resourcing strategy (employees & agents) to drive business performance		■				
	Staff Integrity								33	**Averse** risk appetite for unethical behaviour including staff misfeasance	■					

NB: Changes made are highlighted in blue

KEY	
Risk Appetite	**1**. Averse
	2. Neutral
	3. Tolerant
	4. Seeking
P	**Proximity Risks** : noted by Risk Owners as most current ("proximity"), e.g. potential to impact over the next quarter, and requiring particular attention from Risk Owners
A	**Annual Report** Principal Risks

POL00401624

4.2 Executive Declaration

Author: Deana Herley Sponsor: Jane MacLeod Meeting date: 4 May 2017

Executive Summary

Context

The Post Office Annual Report and Accounts (ARA) includes a statement that the Board has assessed the effectiveness of its risk management and internal control framework. To support this statement management have developed the following processes, Control-Self Assessment (CSA), Weekly Incident Reporting, Whistleblowing, Grapevine (reporting line for Postmasters), Complaints, Internal Audit and Executive Declaration.

The Executive Declaration process supports Group Executive (GE) members considering (and attesting twice yearly), if any additional disclosures are required in our ARA as a part of year-end procedures.

The purpose of this paper is to share the results of the Executive Declaration.

Questions this paper addresses

1. What are the results of the Executive Declaration?
2. What are the next steps?

Conclusion

1. The results have been collated and reviewed for consistency against Internal Audit reviews, Group Risk Profile and Weekly Incident Reporting. 73 items were identified:
   - 3 items of material significance that may impact our going concern assessment and if so, will therefore be disclosed in detail in the ARA re –
     - £950m Working Capital Facility (item 61);
     - Net liabilities provision (item 67); and
     - Uncertainty over future investment from HMG (item 69)
   - 16 items to be disclosed in the Risk section of the ARA re –
     - IT – our dependence on the availability of aging information systems and associated infrastructure.
     - Legal / Regulatory (including procurement) – the legal and regulatory environment that Post Office operates under, which continues to evolve.
     - Change – dependencies, interconnectivities and complexity of changes.
   - 22 items which require an 'accounting judgement' to determine the need for adjustment (shared with Financial Controller for review).
   - 16 items for the attention of RCC members to consider whether any specific disclosure is required.
   - 16 items which are business as usual or not material.

   All items have been summarised in Appendix 1. Items reported at the half year (where there have been no further updates) are included in Appendices 2 and 3.

POL00401624

2. Items agreed for disclosure in the ARA will be presented to the May ARC.

Input Sought

The Committee is asked to review the information provided and:

a) approve the items to be disclosed in the ARA;
b) consider whether the further items described in 1-9, 28-31, 59, 62 and 70 should be disclosed;
c) agree those items which are not material and therefore will not be disclosed; and
d) after consideration of the items raised, determine whether any others should be considered.

POL00401624

Appendix 1 – Items (Q3/4)

Please note:

- The items listed in the table below are possible material items which have been raised by Group Executive (GE) members for consideration for disclosure. Materiality has been defined for the purpose of this exercise as, "qualitatively and/ or quantitatively, as a cut-off point above which something takes on a greater significance and may require a different course of action";
- In deciding how to recognise an item as material, GE members are asked to assess whether it is something that is of a size or impact that would make a difference to the Post Office or our stakeholders, e.g. influence our decision making, cause us significant cost or reputational and/ or regulatory damage; and
- Defined tipping points of materiality used to assess significance where defined, are listed below:

Items	Tipping Point
Risks	Harm Table.xlsx
Frauds, irregularities or losses	£50k or above, which could attract media attention, are systemic/ multiples or have a Network wide impact.
Material contracts	Contracts over £5m or cause significant impact/ harm to the business if they were to go wrong.
Events	Size or impact would make a difference to Post Office or stakeholders.

POL00401624

Statement	Items	GE Member	Action
Material **risks** to Post Office that are not captured in the Group Risk Profile.	**1. Opening hours of branches**. In some cases different from those advertised, especially where the Postmaster is operating non contractual hours.	**Alisdair Cameron**	**RCC to consider whether specific disclosure is required**
	2. An **error in contributions recorded for the defined contribution pension scheme**, the **failure of the Horizon operating system** and the **failure to escalate the BCV fraud**.	**Alisdair Cameron** **Nicholas Kennett**	
	3. 30 December 2016 Cash Sweep Issue. On 30th December, the Treasury team identified that lower than forecast ATM remittances from Bank of Ireland had triggered a gap in available funding. While POL was operating well within its working capital facility, it had requested too small a short-term funding top-up from government. The problem resolved itself on the next working day (Tuesday 3rd January). To avoid either postponing payments to suppliers or going into unauthorised overdraft, the CFO requested the CE, Financial Services and Telecoms, to approach FRES to seek to delay until the following trading day a payment due to FRES, and proposed that cash held by POMS would be swept to POL. Written confirmation was obtained from FRES. The repayment of £12.5m cash to POMS and the delayed payment of £15m to FRES were made on 3 January as agreed. The approvals around the cash swept to POL were not in accordance with requirements under POMS articles or POMS Delegated Authorities. The lessons learnt from this breakdown of control and from failures in the cash flow forecasting process are being fed back to the Board.	**Alisdair Cameron**	
	4. 9 December Credence Duplication Issue. An IT Service alert was issued for an incident involving duplicated Branch data in Credence which was loaded via a batch on December 9th 2016. A root cause investigation with IT suppliers took place to develop a recovery action plan. The majority of payments are based upon Horizon data so were unaffected but there were some instances where Credence data was relied upon for payment calculations. Credence duplication for Bureau (Currency Transactions) and Mails Segregation resulted in the business over paying its Agents. Duplicated data also created issues with key partners WHS and One Stop Stores who are sent weekly reports from Credence automatically to predict their actual remuneration due to be paid in the following month based on December Sales. Following investigation and execution of the recovery plan the impact on the businesses' financials has been remediated.	**Alisdair Cameron**	
	5. BoE Fitness Standards. The Bank of England are introducing new fitness standards for polymer banknotes from the start of 2018. Our High Speed Note Counters cannot be upgraded to meet the standards and therefore need to be replaced. We have a procurement running currently however there remains a risk that the end to end process of procurement, contracting, build and implementation runs into 2018. Being unable to meet BoE fitness standards could risk our NCS status upon which the cash business model of the Post Office is built. In mitigation we have spoken with the BoE and they have indicated that some derogation of the fitness standards would be given however significant delay (more than 3 months) would raise concern.	**Alisdair Cameron**	
	6. Framework for incident reporting. Incidents under £50k, root-cause analysis and remediation are not captured centrally.	**Jane MacLeod**	
	7. PCI accreditation. The business achieved certification of compliance on 28 December 2016. Whilst there is confidence over our continued compliance with PCI, our ability to achieve and maintain accreditation remains a challenge given a change in the Quality Security Assessor due to value of the contract and a number of projects which will impact the scope, such as HNGA EUC Branch rollout, Branch Network rollout and P2PE terminals in Branch. Work is being finalised on	**Kevin Gilliland** **Jane MacLeod** **Rob Houghton**	

POL00401624

Statement	Items	GE Member	Action
	delivery and cost proposition by end of April. Whilst it is not currently expected to be a material item, if the QSA is not appointed by May this starts to cause a concern.		
	8. POCA Modelling Error. Forecasting of Agents Pay should have been 0.125p, however it was rounded to 0.1p. This rounding was a human error for theagent's remuneration team, not a rounding built into the model. The model has been independently validated and we have established that this error does not feed into the funding ask or impact this year's budget. It does however mean that the profitability of the POCA contract over the remaining duration of the contract is £10.9m worse than the modelling suggested. Options to reduce thegap include negotiations with supplier's reductions in agents pay, active migration to alternative accounts etc. are being explored. The options we pursue will depend in large part on the size of the gap we need to close at the end of the procurement (as highlighted at Steerco). A full lessons learnt has also been undertaken.	**Kevin Gilliland**	
	9. Finance (POL FS&T and POMS). An incident arose in January 2017 where it became apparent that there was a lack of consistency between the branch forex holdings asrecorded on Horizon and the reporting in POLSAP. The incident was investigated and a number of anomales were initially identified. Further work identified that the key source of variance was the report being used for analysis. Rectification work is ongoing led by Group Financial Control.	**Nicholas Kennett**	
	10. National Stock Centre Swindon. We have one national stock centre in Swindon whichis the only location from which we serve the branch network with stamps and other stock items. The following should be considered: • The IT is considerably aged and back up requires manual transportation oftapes to an off-site location. There is currently activity under the Back Office Transformation to scope an IT solution for Swindon however a significant failure in the meantime would require manual contingencies to be implemented; these are more labour intensive, increasing cost and potentially slowing service. • The contingency for a site down event in Swindon was to relocate toBirmingham Merlin Coin Centre. Under Simplifying Supply Chain this site has closed. The new contingency is to switch to alternative methods of non-value stock distribution and to relocate value stock to Swansea depot. At this point the contingencies are untested. This will be remedied in the next six months however it does present a risk in the interim. • The financial viability of the current operation at Swindon is predicated on thec. £4m of income we receive for undertaking warehousing services for Royal Mail. The contract is currently under negotiation and should RM decide not to renew, this would reduce the direct income we receive and remove c. £100k of carriage benefits gainedfrom physically consolidating POL and RM items despatched to the same destinations.	**Alisdair Cameron**	**To be disclosed (in Risk note – IT)**
	11. IT Controls Framework is well underway with KMPG. 11 key processes have been identified to be addressed in the first tranche of the project. To date there have been reviews internally and with key suppliers. A number of control gaps have been identified with remediation actons currently being discussed. The IT Security Team are forming the requirements for the Security Operations Centre which will hopefully be established by the end of the year 2017.	**Rob Houghton**	
	12. Cyber Threat. There are a number of Cyber Threat risks which are now managed by IT. We have several risks on the IT register that relate to firewalls, pen testing, applications not supported effectively (i.e. Firefox and Chrome) within the EUC. As the team develops the risks will be mitigated and managed to an acceptable level, one of the key actions for the team is to set up the Security Operations Centre which is expected to be live by the end of 2017.	**Rob Houghton**	

POL00401624

Statement	Items	GE Member	Action
	13. Changes. The closure of banks, and access through our Banking Framework could seesignificant change for the Supply Chain. We have seen bank closures impact branches in different ways; some relatively unaffected whilst others' cash positions move radically (e.g. from c. £2k deficit per week to c. £40k surplus). We don't currently have areliable model for how business banking could impact on Supply Chain. The introduction of Lloyd's business banking could be significant in terms of the amount of coin delivered to branches. We are mitigating this through engagement with the Banking Team.	**Alisdair Cameron**	**To be disclosed (in Risk note – Change)**
	14. OSOP changes. Following the loss of staff in May 2017 there is a significant risk to the delivery of BAU/growth plans and responding to regulatory and competitive pressures. Post Office has not changed its processes or activities, nor implemented a new TOM following the organisational restructure. There is a specific concern about the loss of capacity and knowledge in the Reference Data Team and the impact this may have on key contracts, notably Banking Framework and bill payment, which require reference data changes on an on-going basis. There is a concern that regular mistakes are being made (e.g., TSB transactions as set out in Section 11).	**Nicholas Kennett**	
	15. Card payment rules are evolving and the cost of processing is rising. Visa interchange cap change impacting business to tune of incremental £600k. Working with Visa and Global Payments to divert high value transactions via Visa Me to Me products. Compliance is essential to ensure additional fines are not incurred. The schemes and regulatory bodies regularly update the requirements, and we are currently working under a waiver for certain necessary upgrades to our processing. Changes must be scheduled and the schemes/regulators accept the timescales in order to avoid further costs in the way of fines and/or incremental transactional charges.	**Kevin Gilliland Nicholas Kennett**	**To be disclosed (in Risk note – Legal / Regulatory)**
	16. Vetting issues. In April 2017, POL implemented a general vetting solution. By the end of April, POL will have a vetting solution that covers new starters in FS and Network. A plan is being built across IT, Support Services and other areas to support the delivery of postmaster identification and vetting to support the Banking Framework and regulated POMs sales. Pre solution vetting and training procedures for employees, agents and/or agent employees may not have been consistently applied and/or applied in a way that meets our obligations to other parties (e.g. Banking Framework, POMS and BoI as regulated principals and Royal Mail). A decision will need to be made by GE on whether we retrospectively vet staff who do not meet the new policy / solution.	**Martin Kirke**	
	17. Changes in Discount Rates Applied to Lump Sum Compensation under Insurance Policies. From 20 March 2017 the Government recently reduced the discount rate applied to lump-sum compensation payments awarded to personal injury or fatal accident claimants for future losses. The rate had been set at 2.5% since 2001 and has been reduced to minus 0.75%. This decision is likely to increase costs for insurers who are likely to pass on some of these costs to UK policy holders. A consultation process is being held with insurance industry representatives. At present the full impact of this change is unclear, although it may increase our Employers' Liability and Motor premiums at renewal in September.	**Alisdair Cameron**	**Accounting Judgements**
	18. Reconciliation issues due to timeouts occurring between POL and MoneyGram This could lead to write-offs as there will be differences between MoneyGram and POL figures. At the moment the value is in the region of £750k (reduced from £2.5m due to work conducted at FSC). Work is underway with MoneyGram to close this.	**Nicholas Kennett**	
	19. ATM Maintenance. Supply Chain directly replenish and provide maintenance services to a small number of POL/BoI ATMs. Following Simplifying Supply Chain there are two factors which have reduced our ability to respond to ATM maintenance visits;	**Alisdair Cameron**	**Not Material**

POL00401624

Statement	Items	GE Member	Action
	• By exiting the external CViT market we are no longer in geographical areas as frequently and so unscheduled maintenance services tend to require more system time as we are not 'in the area and passing by'. For some ATMs this can be a four hour round trip from the depot. • We are now a Monday – Friday operation, so should an ATM fail on a Friday evening, it will be out until Monday morning at the earliest. • As a result we have seen availability on CViT service ATMs reduce to around 90% against an ATM SLA of 96%. Poor ATM availability risks reduced use and associated income for ourselves, the BoI and the impacted branches. In mitigation, we have an improvement plan to protect service whilst we explore alternative ways of provisioning these ATMs.		
	20. Johnson Security Ltd. The financial stability of the supplier is a concern. They have been our sole supplier for over 28 years for CVIT vehicle procurement, build and security systems. If Johnsons went out of business, there would only be one other supplier in the market who is untried. Our other preferred supplier withdrew from the market last year (who were supplying Mobile Post Office vans). The supply of these have moved to Johnson Security. Their inability to purchase a £3k part for one of our vehicles prompted us to run an Experian report which highlighted that the financial stability of Johnson's was a risk to us. We have had conversations with Johnson's and various actions have been put in place.	**Alisdair Cameron**	
	21. £1 coin forgeries. Security intelligence suggests that there are a significant number of £1 coin (old and potentially new) forgeries nationally and in particular in NI. Given there is a limited window to launder these coins the possibility that the Post Office network will unknowingly accept these coins is a concern. The Royal Mint's position is that if we continue to demonstrate that we detect some at source they will accept our returns in liner format, weigh check them only and then smelt. However if that decision changes they could decide to forgery detect a sample of our liner returns and apply the percentage to all of our value which could increase the losses we incur.	**Alisdair Cameron**	
	22. Taxes on Staff Entertainment. As part of their Know Your Client review, HMRC have identified that POL has not accounted for tax on staff entertainment. The potential exposure is approx. £30k. Following advice from Deloitte, representations have been made to HMRC that tax should not be due on the basis that the amounts paid by the business predominately relate to, for example, tea/coffee for one-to-one meetings, sandwiches and drinks for working lunches, team meetings etc. and, as the expense typically is limited to no more than £6 per person, the expense is "trivial" and not, therefore, taxable. A response is awaited from HMRC.	**Alisdair Cameron**	
	23. Withdrawal of Extra Statutory Concession for Postmasters HMRC have advised that they will formally withdrawing, from April 2017, the Extra Statutory Concession that allows some postmasters to not have tax paid at source, but Post Office remuneration be treated as trade income. This issue is being dealt with by the Head of Agents' Development and Remuneration.	**Alisdair Cameron**	
	24. Branch conformance with cash declarations has deteriorated in recent years.	**Alisdair Cameron**	
	25. The **SIA's Approved Contractors Scheme** external audit at Manchester and Sheffield units resulted in three 'Improvement Needs' and twelve 'Improvement Observations' being recorded. The following was noted: • The depot operations and the effectiveness of the management team have not yet settled following transition. • Gaps in management controls identified via internal audits. • Gaps in checks and record keeping being addressed via internal audit action plans, with support from H&S team.	**Alisdair Cameron**	

POL00401624

Statement	Items	GE Member	Action
	Action plans are in place to address the findings at both sites; some actions have already been completed whilst others have longer timescales, for example where formal training or additional resource is required. A senior operational manager has been assigned to the depots on a temporary basis to support them deliver their actions, working jointly with H&S team to ensure central actions are closed and to support depots with local actions. The External Auditor will conduct a follow up audit in 12 weeks, specifically to ensure that the H&S elements of the Improvement Needs have been addressed.		
	26. Postal redirection from 148 Old Street expired. As a consequence, c.6 envelopes containing Suspicious Activity Reports were opened and redirected to Finsbury Dials, including one envelope that was empty when received. It is unknown what else has been impacted.	**Jane MacLeod**	
	27. Payments risk competitive threat and impact of market developments Co-op withdrawal from the payments re-seller market underway. Total impact potential 11m transaction £2.8m estimate overall but realistic retention of volume via Allpay.	**Nicholas Kennett**	
Material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners.	**28. Losses are c. £4m worse than budget at p10** (updated for year-end). As reported, due to agent debt provisions and the BCV fraud in particular CViT robberies, as reported, have increased to £278k at P10 versus £123k in the full year 2015/16.	**Alisdair Cameron**	**RCC to consider whether specific disclosure is required**
	29. Frauds. A number of frauds have been reported during the period, including further instances of the BCV fraud, which had a further unsuccessful attempt in October. Frauds have also been identified around Santander, MoneyGram, Transcash and 'deferred check-in service'.	**Alisdair Cameron**	
	30. Passports. A number of passports were lost when inappropriately sent in the normal post from the Belfast depot. The DWP has been informed.	**Alisdair Cameron**	
Complex or subjective **accounting judgements**, **estimates and revenue transactions*.**	**31. Value Share Agreement with Bank of Ireland (BoI).** In May 2016 an agreement was entered into with BoI where Post Office received a guaranteed minimum savings commission in 2016/17; additional savings commissions according to a formula based on the to the Net Interest Margin on that book of business; and Additional Commissions for the development of the Savings business. BoI was granted an extension to the run-off period that would apply in certain circumstances at the end of its contract with Post Office. The computation of the amounts receivable is not subject to judgement, but the amounts are material and one-off in nature.	**Nicholas Kennett**	
	32. Material accounting judgements. These are set out in the March ARC paper.	**Alisdair Cameron**	**Accounting Judgement**
	33. Banking services deferred income. Historical balances relating to banking services income totalling £2.2m, which are under review by financial accounting to confirm whether the income should continue to be deferred.	**Nicholas Kennett**	
	34. Bill Payments. We have agreements in place with a number of clients whereby the Post Office receives commission when members of the public settle their bills with these clients at the Post Office. The timing of payments and settlements means that an accrued income balance (asset) would be expected, but historically this has been a liability c£4.5m. A preliminary review was undertaken into the bill payments journal process and corresponding Balance Sheet entry. Any decision to release all or part of that balance could have a significant positive impact on profits for the period. A £1m per month *4 mths has been released back into the P&L.	**Kevin Gilliland**	
	35. Private Healthcare (budgeted ~£0.5m, spent ~£1m) The current policy is based on paying for medical treatment. The value of this payment is dependent on the number of claims and cost of treatment. It doubled due to deficit from previous years, increase in claims during restructure	**Martin Kirke**	

POL00401624

Statement	Items	GE Member	Action
	and high-value cases. It is proposed that a procurement process is launched with the aim of implementing an insured scheme.		
	36. Group Income Protection & Life Assurance (from ~£0.4m to ~£3m) Premiums are based on risk profile of POL employed population and calculated by external underwriters who base it on events beyond POL control (e.g. health issues). Premium increased due to population increase after transferring in people from DB to DC. Also, risk profile of those transferring in is greater.	**Martin Kirke**	
	37. Carrying value of the business acquired under Project Hawk The carrying value in the books of POMS of the business acquired under Project Hawk is £43.9m. In order to retain this carrying value, an impairment revenue must be carried out to demonstrate that the future value of the business acquired exceeds the carrying value. An impairment review prepared and presented to the POMS ARC in March 2017 confirms that to be the case.	**Nicholas Kennett**	
	38. Accounting treatment of BISL/Junction income and costs in POMS. The accounting treatment adopted is to state the income and costs of POMS arrangement with BISL/Junction gross, with no netting-off. However, there are alternative accounting treatments which would involve netting these off, for instance, if it was viewed as a joint undertaking. The treatment remains consistent with that adopted for the 2015/16 financial statements. The potential impact of netting-off would be to reduce both income and costs by c£2m in 2016/17, but would not impact EBITDAS.	**Nicholas Kennett**	
	39. Banking services deferred income. Historical balances relating to banking services income totalling £2.2m, which are under review by financial accounting to confirm whether the income should continue to be deferred.	**Nicholas Kennett**	
	40. Contractor Uplifts / IR35. Legislation will come into force which will result in greater contractor cost to POL. Contractors are important to deliver change.	**Martin Kirke**	**Not Material**
	41. Project Peregrine (Exceptional). As part of Post Office's Transformation governance, I am responsible for exceptional spend in Project Peregrine (the nature of which is strictly confidential and subject to an NDA) totalling £2.3m in 2016/17.	**Nicholas Kennett**	
Changes to **accounting policy.**	**42. Potential changes to the accounting policy.** For investments in joint ventures and to accounting estimates for the impairment of fixed assets are set out in the ARC judgement paper.	**Alisdair Cameron**	**Accounting Judgement**
Provisions or **exceptional items.**	**43. Postmaster compensation**. The main judgement on provisions relates to the financial value of the provision for postmasters compensation. We expect to disclose a contingent liability in the 2016/17 financial statements in respect of Postmaster litigation. We do not currently have clarity around the amount of the claim. A third party is currently reviewing the accounting for control and suspense accounts.	**Alisdair Cameron** **Jane MacLeod**	
	44. Onerous Contract Provision Value @ P11 - £9.0m	**Alisdair Cameron**	
	45. Vacant Leasehold Provision Value @ P11 - £12.6M	**Alisdair Cameron**	
	46. Provisions for Life insurance commission clawback and Remark. POMS carries provisions totalling £2.1m in respect of commission clawback on cancelled life insurance policies and also for historical claims from Remark in respect of direct mailing success fees. The calculation of these provisions is subjective, but based on the experience of the business to date they are considered sufficient to meet future liabilities.	**Nicholas Kennett**	
	47. Telecoms bad debt provision. Bad debt provision exists in relation to amounts due from telecoms customers. The criteria is that aged debts over 90 days are fully provided for.	**Nicholas Kennett**	

POL00401624

Statement	Items	GE Member	Action
Liabilities and contingencies, including those associated with guarantees*.	**48. HMRC fine on registration of premises.** We have been advised that HMRC is to issue a pre-penalty notice to Post Office for £985k in relation to the historic failure to file notifications of changes of premises at which regulated activities occurred. Moneygram is dependent on Post Office to notify it of changes to premises so that it can maintain its own registrations with HMRC. It is possible that Moneygram, could seek to recover the amount of any fines or penalties from Post Office, should they be levied against Moneygram by HMRC.	**Alisdair Cameron** **Jane MacLeod**	
	49. Dilapidations Liability. This forms part of Onerous and Vacant LH provision amounts are £1.8m and £4.8m respectively and are part of the provision amounts in the above section. The amounts provisioned are based on an actual dilapidations assessment where lease is about to be surrendered or 80% of the rental value if the lease has several years to run. Actual settlements can vary, as soon as this is clear the provision value is amended. **BAU Dilapidations Provision**. £248k covering unsettled dilapidation settlements for BAU element of the portfolio that is not programme related.	**Alisdair Cameron**	
	50. Energy MPANs (Meter Point Administration Number) not assigned to POL (6 Sites). A liability exists for electricity that has not been billed to POL due to the MPANs not being assigned to us and little is known about the energy providers, energy has been consumed by POL. As at P12 this is not provided for, based on CBRE information and subject to high level checks by POL energy analyst the liability if industry standards are applied is £0.3m, liability if taken to statutory limitations £0.6m.	**Alisdair Cameron**	
	51. Future Walk Fuel Remediation. A £250k provision exists currently within the property accounts for the POL share of the fuel remediation works that continue to take place at the Future Walk site, our legal team have yet to receive confirmation that no approach for payment by RML will be made.	**Alisdair Cameron**	
	52. HMRC has informed Post Office, through the Post Office GC and MLRO that there are instances where we have not met our AML regulatory duties for Travel Money (and possibly Bill Payment), foreign exchange and MoneyGram and gift cards. This has been reported centrally. This may result in Post Office incurring penalties and remedial costs; details have not yet been determined by HMRC: **Regulation 20 -Policies and Procedures:** • No risk assessment of "normal and expected" FX transactions • POL Risk assessment shows current overall FX controls as "ineffective" **Regulation 7-Application of customer due diligence measures:** • 26K transactions have mandatory data capture which appears to have been overridden or data lost **Regulation 8 -Ongoing monitoring:** • Breaches of due diligence thresholds not captured by central monitoring • Not identifying potential business relationships • PEP and Sanctions checks not applied **Regulation 19 -Record-keeping:** • 26K transactions have mandatory data capture which appears to have been overridden or data lost • Unable to identify what and where due diligence information held **Regulation 21 –Training:** • Failure to train non branch staff prior to 2016	**Jane MacLeod** **Nicholas Kennett**	

POL00401624

Statement	Items	GE Member	Action
Any material **legal action** being taken by or against PO.	**53. Choice International.** This company has demanded Post Office repay £215,927.88 of VAT which Choice claims was incorrectly charged for Post Office Supply Chain services. Post Office has declined this refund, but offered to consider seeking repayment of the VAT through HMRC under section 80 of the Value Added Tax Act 1994 if indemnified to do so by Choice.	**Jane MacLeod** **Nicholas Kennett**	**To be disclosed (in Risk note – Legal / Regulatory)**
	54. Non-compliance with PCR. There are a number of contracts signed or extended which were not procured or extended in line with Public Procurement Regulations 2015. They are generally low risk and with a commercial imperative. New controls have been introduced to record incidents or exceptions going forward. This will bring greater clarity over level of non-compliance with PCR.	**Jane MacLeod**	
	55. Global 365. This is a company that sought to work with Post Office for Smart Metering in the emerging energy market. Discussions were terminated by Post Office after exploring all possible avenues but Global 365 continue to display the Post Office logo on their website as a partner. Logo still remains and letter to be issued by Legal.	**Kevin Gilliland**	**Not Material**
Any **legislative, regulatory or contractual compliance issues** that have come to light.	**56. Telecoms cyber-attack.** Post Office Broadband business and c.108 thousand customers suffered a cyber-attack (DDOS or "BOT" attack) at the end of November 2016. This was part of a global attack. This led to customer either being denied service or having service speeds significantly reduced for a period of 3-6 days. A fix was quickly implemented but additional contact centre costs for extended hours were incurred (c £100,000). Minimal customer claims were made (338 for £1,500 in total). The attack was reported to the Post Office RCC & ARC. However, this has resulted in Post Office rising to number two in the published Ofcom complaints table in Q4 2016/7 and we expect this to impact also on Post Office's position in Ofcom's industry table on call response times yet to be published.	**Nicholas Kennett**	**To be disclosed (in Risk note – IT)**
	57. Enterprise Act. Legislation proposing to cap redundancy payments at £95k. This will impact POL ability to manage change through VR.	**Martin Kirke**	**To be disclosed (in Risk note – Legal / Regulatory)**
	58. Commercial risk from Ofcom intervention in standalone landline telephone service Ofcom is consulting on a number of remedies to increase customer switching and reduce price paid by consumers in this market. The proposed remedies are only targeted at BT and are expected to be implemented early in 2018, but include a potential £5 per month reduction in Line rental charges, which if Post Office choses to respond may impact the Post Office home phone only business. We looking to mitigate this risk by participating in the consultation process, and refining our customer propositions, however the potential impact in FY 16/17 could be a reduction of £45k - £3m depending on the exact remedies and POL strategic response.	**Nicholas Kennett**	**To be disclosed (in Risk note – Legal /Regulatory)**
Material **new contracts or extensions** entered into, **direct awards** and where I have not followed the **contract process.**	**59. The business does not have a complete suite copy of contracts.** The Legal Team are working to collect, summarise and store all contracts in a central repository through the Bravo procurement system.	**Jane MacLeod**	**RCC to consider whether specific disclosure is required**
	60. Non-compliance with PCR. Over the last 6 months and prior to this, POL has entered into a number of contracts that have been direct awards and not compliant with PCR. Some have been for professional, where the nature of the services or the timetable for completion have been commercially or operationally sensitive. Some have reflected short-term, tactical contract extensions to allow for fully compliant procurement processes to be run with detailed contract requirements where the business is changing direction. Procurement has identified that a written risk note has been prepared by legal and signed by appropriate stakeholders as part of the contract approval process.	**Jane MacLeod** **Mark Davies** **Nicholas Kennett**	**To be disclosed (in Risk note – Legal / Regulatory)**

POL00401624

Statement	Items	GE Member	Action
Obligation breaches on material **contracts** that I am sponsor for*.	**61. £950m Working Capital Facility – Reporting Requirement.** Under the £950m working capital facility provided by BEIS there is an information requirement to provide weekly reporting of security headroom. During the year we agreed with BEIS that, due to systems constraints, we would provide monthly rather than weekly reporting. This was agreed informally at a face-to-face meeting with BEIS (James Baugh – UKGI) and then confirmed by email. No amendment to the agreement has been made. All monthly reports have been provided for FY16/17 (to P11).	**Alisdair Cameron**	**To be disclosed**
	62. Camelot. Post Office are Camelot's only retail partner that can pay mid-tier prizes (£501 - £50,000) to customers. We deliver this service through Horizon paying 68,027 prizes to the value of £111m in 2016/17, this generated £700k for POL. The Gambling Commission are putting pressure on Camelot to have tighter controls on mid-tier prize payments which need to be meaningful and with possible financial penalties. A pilot audit was introduced as part of an informal agreement (not contractual). This involved self-auditing 95 branches by desktop and 5 physical branch audits each quarter. It is apparent that the results given to Camelot, of the first 2 pilot audits in Q3 & Q4 misrepresented audited performance by excluding one element that would have significantly (by c60%) reduced the result if included. This has been rectified for the most recent audit which has yet to be shared with Camelot. We believe that the pilot audit results have not been shared with the Gambling commission. We will be having an independent review of the product which will cover contractual obligations, risks and KPI programme. We are also proposing a strategic review of the product from both a market and proposition perspective.	**Kevin Gilliland**	**RCC to consider whether specific disclosure is required**
	63. Contract Obligations and Risks. There is an incomplete understanding of obligations and risks associated with out of contract suppliers. Legal has introduced an obligations spreadsheet within the Legal Risk Note to assist the business in managing its obligations. However compliance with the requirement cannot be verified.	**Jane MacLeod**	**To be disclosed (in Risk note – Legal / Regulatory)**
	64. Banking Framework. Royal Mail continue to disappoint delivering cheques late to IPSL. This means the banks complain about the fact they are paying for the framework, but not getting a good cheque delivery service. Mitigating actions being put in place to get RM to undertake urgent improvement (to achieve basic SLA commitments).	**Nicholas Kennett**	**Not Material**
	65. Banking Framework - Service stability/incident risk. ATOS service delivery and roll-out of new services has been below banking framework requirements. In the last quarter two specific incidents have occurred: • In launching a model office-only test update, ATOS removed TSB for manual deposits (c.200 transactions that would normally have succeeded were unable to be processed)and switched on Bank of Scotland several weeks ahead of plan – both of which happened across the entire network. Five live transactions were accepted that cannot be completed and need to be refunded. • In enabling the BCV Fraud fix in January 2017, existing'back door' routes were left open for BoI, which meant launch day confusion for postmasters, customers and our banking clients who continued to receive transactions that should have been blocked. • There are a number of routine issues like this that require significant intervention to protect us operationally and reputationally, with the commensurate impact on bank partner confidence that Post Office is able to handle multiple complex services in a robust and scalable manner.	**Nicholas Kennett**	
Gifts and hospitality which have not been	**66. Reporting of gifts and hospitality.** Reporting levels are low and therefore we cannot be certain that reporting guidelines are met. Many approvals are retrospective.	**Alisdair Cameron**	

POL00401624

Statement	Items	GE Member	Action
approved and registered in accordance with policy*.			
Material events that could **crystallise** before the end of the reporting period above.	**67.** Post Office will go negative on our balance sheet subject to accounting treatments.	**Jane MacLeod**	**To be disclosed**
	68. Change. There is a risk that change is not managed effectively and efficiently due to two main drivers: • The change delivery model and the ATOS SIAM operating model which add complexity and overhead to delivering change. • The inability of POL to effectively manage suppliers from both a technical andleadership perspective. The IT Portfolio Office Manager is now in situ and discussions are taking place (Project Armada) to insource key IT services which will enable POL to establish a Portfolio Office which enable PO to effectively and efficiently manage the Change portfolio.	**Rob Houghton**	**To be disclosed (in Risk note – IT)**
Any **other information** that could have a material impact on the period (indicated above).	**69. Funding.** Our future investment funding from HMG remains unresolved, and if this continues beyond May we face significant risks, in particular: a) insufficient time to complete the state aid approval process prior to the start of 2018/19; and b) an inability to plan effectively on the implementation of our strategy.	**Alisdair Cameron Martin Edwards**	**To be disclosed**
	70. Payments Term down to 30 days from 45. There will be statutory duty to report on payment practices and performances coming into effect on 6 April 2017, will Post Office required to report on or before 30 October 2018 for the period 1 April 2018 – 30 September 2018. Non-compliance will be a criminal offence by the company and every company director although it will be a defence if the director took reasonable steps.	**Alisdair Cameron**	**RCC to consider whether specific disclosure is required**
	71. New Money Laundering Regulations. This comes into force 26 June 2017, are expected to require fit and proper tests to be undertaken for managers and agents, it is notyet clear whether this will include managers and staff in Directly Managed branches, postmasters and their assistants. Nor is there yet guidance on if Post Office will be required to retrospectively undertake these tests for existing managers, staff and agents. If this does happen the impact will be material. This also introduces a number of challenges for our gift card product. Implications are not yet fully understood, but in the worst case scenario customer KYC procedures would need to be undertaken for every card purchase.	**Jane MacLeod Nicholas Kennett**	**To be disclosed (in Risk note – Legal / Regulatory)**
	72. Recent incidents of missing data from Accenture This is resulting is misbalancing between Horizon and Client data. Each incident is followed up and the missing files are loaded but highlights current IT issues facing FSC.	**Alisdair Cameron**	**Accounting Judgement**
	73. Retail Sales Awards. This is currently unbudgeted activity. We are seeking sponsorship to cover the costs of the event (approx. £400k). There is a budget risk if this does not come to fruition.	**Mark Davies**	**Not Material**

POL00401624

Appendix 2 – Watch List Item (cont. Q1/2)

Statement		Items	Owner
Material **risks** to Post Office that are not captured in the Group Risk Profile	**1**	The **Group Risk Profile** discussed at the RCC and ARC is necessarily focussed at a high level. However there are lesser risks, and/or more granular risks within these categories that have the capacity to impact Post Office adversely should they crystallise, and there is as yet limited oversight of these lesser risks and the factors that could cause them to deteriorate.	**Jane MacLeod**
	2	**Reconciliation issues due to timeouts occurring between Post Office and MoneyGram**. These could lead to write-offs (as well as customer/postmaster impact) as there will be differences between MoneyGram and Post Office figures. At the moment the value is in the region of £2.5m but it is expected that the vast majority will be cleared.	**Nicholas Kennett**
Any **legislative**, **regulatory or contractual compliance issues** that have come to light	**3**	**Branches report incidents of non-compliance on a case-by-case basis.** KPIs do not cover failures to comply with Post Office policies and procedures (inclusive of data protection controls).	**Jane MacLeod**
Material breakdowns of internal control, breaches or significant non-compliance with internal and external guidelines, including of the **General Control Framework** and **policies** that I am accountable for	**4**	**Credit Card Balance Limits (August 2016).** BoI have to declare the amount of balances it will hold to the FCA. In August, BoI declared that it had balance sheet issues in that overall credit balances were in danger of exceeding formal business limits. Consequently, Post Office had to slow down our sales so balance limits were not exceeded whilst they waited formal sign off on increased limits. This resulted in the majority of our online paid for activity being stopped which saw sales volumes more than half. Going forward, sales targets will be by product type rather than overall sales volumes. There is a risk that if balance limits are not high enough then we will have to slow down sales again.	**Nicholas Kennett**
	5	A breakdown in process occurred when a customer sent in multiple batches of **Postal Orders**; the FSC returned a cheque for the amounts sent in. This has been referred to Legal and the SFO due to the nature of the individual's business but also as we returned a cheque in his name and the Postal Orders were made payable to his company. The customer continues to request we continue the service, but instructions have been given that existing process requirements should we followed.	**Nicholas Kennett**
Material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners.	**6**	Losses are c. £2.8m worse than budget in H1, as reported, due to agent debt provisions and the BCV fraud. CViT robberies, as reported, have increased to £187k in H1 versus £123k in the full year 2015/16. A number of frauds have been reported during the period, including further instances of the BCV fraud, which had a further unsuccessful attempt in October. Frauds have also been identified around Santander, Moneygram and Transcash.	**Alisdair Cameron**
	7	A potential risk has recently arisen whereby the **FSJVA and associated contracts may not allow Post Office to give BoI third party lead data for outbound contact centre follow up.** Examples include (1) Horizon leads, (2) Data driven lead generation programme. FS are working with ISAG to clarify the situation.	**Nicholas Kennett**
Complex or subjective **accounting judgements**, **estimates and revenue transactions***	**8**	We are currently debating with our external auditors the **correct accounting treatments for the closure of the third party CViT work and the closure of the defined benefit pension scheme.**	**Alisdair Cameron**
	9	We are about to **kick off a review of our accounting policies with EY.**	**Alisdair Cameron**
Material **legal action** being taken by or against PO	**10**	**Appointments of regulated entities as agents** constitutes a regulatory breach and a breach of the AR arrangements with each of BoI and POMS as principal. Disclosure has been made to each of BoI and POMS.	**Jane MacLeod** **Kevin Gilliland**

POL00401624

Appendix 3 - Items for Information *(cont. from Q1/2)*

Statement		Items	Owner
Material **risks** to Post Office that are not captured in the Group Risk Profile	**1**	There are a **significant number of projects and other initiatives running concurrently**. Without careful resource planning there is a risk that one or more of these projects/initiatives will be delayed, run over budget or fail to deliver the anticipated benefits.	**Jane MacLeod**
	2	If we **re-purpose the remaining Network Transformation funds** , there is the risk of still having to pay compensation that we may have already spent elsewhere.	**Kevin Gilliland**
	3	The risks associated with **ATM attacks**.	**Nicholas Kennett**
	4	**Notice of sums in arrears (NOSIA)** is sent to customers after they miss two payments. The customer must make the minimum payment (2.5%). However, if a customer had set up a direct debit (DD) for more than the minimum payment the NOSIA stated, the fixed DD amount rather than the minimum payment. This impacted the printed NOSIA which is a legal document but interest charges and payments were applied correctly to the account. Therefore the NOSIA was not legally binding. Cheques were sent to customer with a refund of default fees and charges accrued since the incorrect NOSIA was sent. Compensation was also given. New NOSIA was sent along with the cheque. *October 2008 to Dec 2015. Issue raised Feb 2016. Circa 4,000 customers impacted.*	**Nicholas Kennett**
	5	BoI identified that an **error occurred when calculating the refund and compensation amount** which was sent to impacted customers in April / May 2016. BoI elected to pay discretionary compensation of 2.6% of the refunded default fees and interest was added to the remediation amount. However this was calculated as simple interest (based on the overall refund) rather than being calculated on an annual basis. Therefore customers who had been impacted over a longer period should have received further compensation. The date the refund of fees and charges began was set as two months after the impacted customers received their incorrect NOSIA, this should instead have been calculated from the date the incorrect NOSIA was issued. New letters and cheque refunds are to be issued to impacted customers. *April/May 2016. Issue raised October 2016. Circa 2,000 customers impacted.*	**Nicholas Kennett**
Any **legislative**, **regulatory or contractual compliance issues** that have come to light	**6**	**Appointments of regulated entities as agents** constitutes a regulatory breach and a breach of the AR arrangements with each of BoI and POMS as principal. Disclosure has been made to each of BoI and POMS.	**Jane MacLeod Kevin Gilliland**
	7	We have had one complaint from the Advertising Standards Authority as to potentially **misleading marketing communications in Post Office broadband advertising** . The matter has been clarified with the ASA and the relevant advertising campaign is in any case no longer being run. The issue appears to have been in relation to the expression "unlimited broadband"; unlimited does not mean unlimited as to speed.	**Jane MacLeod**
	8	A potential risk has recently arisen whereby the **FSJVA and associated contracts may not allow Post Office to give BoI third party lead data for outbound contact centre follow up.** Examples include (1) Horizon leads, (2) Data driven lead generation programme. FS are working with ISAG to clarify the situation.	**Nicholas Kennett**
Material **frauds**, **irregularities or losses** that have come to light, whether carried out by our staff, agents, contractors, suppliers or partners.	**9**	A handful (c.5-10) of **cheque fraud instances** on Post Office Current Account across Q1. Customers withdrawing funds before cheque outcome is known, due to delays in cheque clearing process between Post Office and BoI. Value less than £50k. This matter is on the FS team's risk log and Post Office / BoI have jointly put mitigating actions in place.	**Nicholas Kennett**
Complex or subjective **accounting judgements**, **estimates and revenue transactions***	**10**	We are in the process of **changing payment calculation methodology with Santander**. This will see two changes: 1) moving from payment against a forecast, to payment against actuals. This will add certainty and reduce our exposure to the £300m overnight CAP. We are also moving to a DAY D settlement for Bill Payments, which will increase our exposure, but will reduce our requirements for working capital each day against the £950m lending facility. The net-net of these changes is that we will potentially move from a worst case overnight debt position of c£180m to a slightly higher level (c. £200-210m), but still be significantly below the headline CAP of £300m, with a corresponding improvement of that much in our working capital limit.	**Nicholas Kennett**

POL00401624

Statement		Items	Owner
New contracts or extensions entered into, **direct awards** and where I have not followed the **contract process**	**11**	The original contract with Ingenico expired in March 2012 however the maintenance of the devices continues to be procured on an annual rolling basis on standard purchase order terms. The current contract expires 31st March 2017 after which Ingenico have confirmed they cannot be supported. In FY 2016/2017 and 2017/2018, Post Office continues to develop its Branch Technology (EPOSS integration or Thin Client Application) and Payment strategies which will become the long term strategic replacement of the existing Paystation service. Between 1st April 2017 and 31st March 2018, Post Office requires an extension to the existing Ingenico contract to protect the existing service until an alternative strategic solution is delivered. We are currently investigating the compliant procurement status of a 1 year extension. New procurement regulations issued in 2015 does introduce a risk of challenge which is set out in s CMS legal advice note. A Risk Acceptance Note is drafted.	**Alisdair Cameron Nicholas Kennett**
	12	**A 1 year extension was made in May 2016 for Salesforce software** . The **original contract in 2012 was believed not competitively procured** in accordance with procurement regulations. The value is £686K.	**Alisdair Cameron**
	13	KPMG and Macquarie support for Projects Peregrine and Falcon did not go through the public procurement process, but was subject to a confidential competitive bid process and was approved by the TSG/CFO.	**Nicholas Kennett**
Obligation breaches on material **contracts** that I am sponsor for*	**14**	Obligation breach by **ATOS non-conformance in respect of Service Desk fulfilment** (SISD agreement Schedule 2.1)	**Alisdair Cameron**
	15	Santander did have a claim regarding the **non-conformance of cheques accepted over our counter for bill payments** (such as not made payable to Post Office or not signed etc.). This is issue has been closed in principle and a new contract is expected to be signed in November which clarifies that Post Office bears no obligation for returned cheques.	**Nicholas Kennett**

POL00401624

3.3)Risk Submission for the Annual Report and Accounts 2016/17

Author: Victoria Moss Sponsor: Jane MacLeod Meeting date: 4 May 2017

Executive Summary

Context

A report from the Audit, Risk and Compliance Committee (ARC) forms part of the corporate governance statement in the Annual Report and Accounts (ARA) and is followed by *Management of Risks* and *Our Principal Risks and Mitigations.* This extract of the draft corporate governance statement is appended to this paper for review and for approval of its onward submission to the ARC, as part of the full ARA.

The *Management of Risks* and *Our Principal Risks and Mitigations* sections of the ARA are a product of the risk team, in particular the work set out in the papers *Top Risks* and *Executive Declarations*, also provided for the RCC's consideration.

Questions addressed in this report

1. Are the principal risks as set out in the draft ARA extract the correct risks for inclusion and are the descriptions of those risks appropriate?
2. Are there any amendments to be made to the draft ARA extract on audit and risk prior to its submission to the ARC?

Conclusion

1. Those principal risks set out in the draft ARA were considered by the risk team, at the time of drafting, to be the correct risks for inclusion and to have appropriate descriptions.
2. No amendments to the draft ARA extract on audit and risk are proposed by the risk or CoSec teams.

Input Sought

The Committee is asked to provide comments on the draft audit and risk submission for the ARA 2016/17, in particular on the principal risks, and to approve onward submission to the ARC.

Appendix

Audit and risk extract from the draft Annual Report and Accounts 2016/17

POL00401624

Committees

To assist in the execution of its corporate governance responsibilities, the Board has established a governance structure of three committees which deal with specific topics requiring independent oversight, specifically: audit, risk and compliance; nominations; and remuneration. Each committee is chaired by a Non-Executive Director.

The Board delegates certain authorities to these committees which operate within their own agreed, documented Terms of Reference. The Terms of Reference for the Audit, Risk and Compliance Committee were last reviewed by the Committee and approved by the Board in September 2015. The Terms of Reference for the Nominations and Remuneration Committees were last approved by the Board in March 2015 and reviewed in November 2015. The annual review carried out in March 2017 confirmed that each committee had delivered against its Terms of Reference during 2016/17.

Terms of Reference for the committees are available on the Post Office website [add link].

Audit, Risk and Compliance Committee

Role and Membership

The Committee is chaired by Carla Stent, and the other members are Ken McCall, the Senior Independent Director, Richard Callard and Tim Franklin, both Non-Executive Directors. The Board considers that the Committee's members have broad commercial knowledge and extensive business leadership experience and that this constitutes a broad and suitable mix of business and financial experience and expertise.

The Head of Risk and Assurance or the Senior Internal Audit Manager attended all but one of the meetings of the Committee and also met the Committee Chairman, as required, through the year. The external auditor was invited to attend meetings of the Committee as appropriate.

Further detailed information on the management of risk within Post Office, together with identification of principal risks, their impacts and mitigation, can be found in the Management of Risk section on pages XX.

Work carried out by the Committee in 2016/17

During the year, the Committee reviewed the annual report and financial statements for 2015/16, including consideration of principal and strategic risks, and recommended Board approval. The Committee oversaw the further progress towards full implementation of the Group-wide Risk Management Framework, including consideration of additional forms of self-assessment for management and increased consideration of financial services risk to support the development of the financial services strategy. The Committee approved the annual audit plans for the internal audit function and Ernst & Young LLP, the external auditors.

The Committee also reviewed the work carried out by risk management, internal audit and by the external auditor, further details of which can be found below. It received regular reports on particular risk areas, including business transformation, financial conduct, money laundering, cyber & information security (including data protection) and pension risks. The Committee has also monitored the potential impact on the business of Brexit. These considerations enabled it to complete its year-end annual assessment of the effectiveness of risk management and internal controls, on behalf of the Board.

POL00401624

2017/18 Forward Focus

During 2017/18 the Committee's planned focus would include oversight of the progress with improvements in Financial and IT controls. In supporting delivery of the strategy for expansion in financial services the Committee would be receiving updates on developments in financial services product legislation.

Annual Assessment

To complete its annual assessment of the effectiveness of risk management and internal controls, the Committee considers the: risk management framework; systems of internal control; and preparation of the annual and interim financial statements and a review of the nature and scope of the external audit.

In consequence, the Board, through the Committee, confirmed that there is a regularly reviewed ongoing process of identifying, evaluating and managing the principal risks faced by Post Office and their related controls. The process has been in place for the year under review and up to the date of approval of the annual report and financial statements. The Board has reviewed its effectiveness and conclude that they provide reasonable, but not absolute, assurance, against material misstatement or loss.

Internal Audit

Internal Audit provides the Committee with assurance over Post Office's key risk areas. To maintain independence, the Head of Internal Audit reports functionally to the Chairman of the Committee and operationally to the General Counsel. Assurance is achieved through a mixture of in-house auditors, supplemented by a co-sourcing arrangement for more specialist, one-off expertise and assurance over significant change programmes.

The annual plan is developed by Internal Audit across the risk universe with input from management. It is approved by the Committee and may be updated, with the Committee's consent. Updates and findings are provided by the Head of Internal Audit at each meeting. Any significant findings or identified risks are closely examined to confirm that appropriate action is being taken. During the year, Internal Audit conducted reviews across a range of business areas including financial services and business transformation.

A self-assessment of compliance with the Internal Audit Charter was conducted at the end of the year and reviewed by the Committee.

External Audit

The external auditors discuss with management the reporting of operational results and the financial condition of the Post Office and present their findings to the Committee.

During the year the external auditors met once with the Committee in the absence of the executive. The Committee agreed the external audit fee and considered the external auditors to have an appropriate level of independence. Prior to the end of year a change in the external audit partner provided enhanced levels of independence.

During the year XX% of the total fees paid to Ernst & Young were for non-audit services, an increase/decrease on the 19% paid in 2015/16.

POL00401624

Management of Risk

Our Approach to Risk

We define risk as anything that can adversely affect our abili ty to meet the Post Office's objectives, maintain its reputation and comply with regulatory standards. We seek to understand and harness risk in the pursuit of our aims and business plan objectives. As we progress, our aim is to operate within an acceptable level of risk taking.

Risk Management Governance

The Board is accountable for the risk management and internal controls in the Post Office, for reviewing their effectiveness and for determining the nature and extent of the principal risks. Responsibility for day -to-day operations rests with members of the Group Executive. The Risk and Compliance Committee reviews the effectiveness of the risk management framework and management of the principal risks. The committee is chaired by the General Counsel, membership includes all of the Group Executive and the output is reported to the Audit, Risk & Compliance Committee (ARC).

Assurance for the Board is provided by the Audit, Risk and Compliance Committee, through review of reports from Management, Risk, Internal Audit, external advisers and External Audit.

Our Risk Management Framework

The PO risk management framework includes risk governance, risk identification, measurement and management, and risk reporting and set out the 'top-down' and 'bottom-up' approach to risk identification for the PO. Material and e merging risks are identified through a process of regular structured dialogue with subject -matter experts across the business.

The PO approach to risk management is based on the underlying principle of line management accountability for effective implementation of internal controls to manage risk. Details of our Principal Risks are included on page ZZZ.

Internal Control Framework

We have an internal control framework in place in relation to our financial reporting processes, which falls under our self -assessment regime. Further work is currently underway to develop a similar framework for our IT controls. Our risk management efforts are also underpinned by our General Control Framework and Executives' Declaration.

The Board has put in place an organisational structure with formally defined lines of responsibility and delegation of authority. Executive Management have established procedures for setting our direction, planning and controlling the operation of our business, and reviewing and monitoring our performance and conduct.

Progress during the year and plans for next year

During the year, we have continued to develop our risk management capability. Highlights of what's been achieved and what is planned for next year include:

Risk assessment: during 2016/ 17, there we improved the the risk management framework and its use in the business areas and by RCC. We also developed incident reporting and formalised risk exceptions process to provide lessons learnt on our risk assessments and operatio nalise our risk appetite further.	**Risk assessment:** for 2017/ 18 we aim to improve our understanding of the nature of risks that POL faces and continue to improve oversight of the level of risk actually being taken across PO and the effectiveness of the mi tigating actions.
Control environment: during 2016/17, we have formalised our monitoring mechanisms for General Control Framework including remediation activity and embedded a Control Self -Assessment across fifteen of our key processes.	**Control environment:** for 2017/18, we plan to roll out a reporting tool which will be used to monitor the risk and control environment for each business unit under our self -assessment regime.

POL00401624

Our Principal Risks and Mitigations

These are our principal risks, detailed with their potential consequences if they were to crystallise and how the Post Office manages them. Any of these risks could have a material impact on our results, condition and prospects. However, these risks should not be regarded as a complete and comprehensive statement of all potential risks; some risks are not yet known and some that are not considered material could later turn out to be material.

Potential risks	Consequences	Key Mitigations
STRATEGIC RISKS		
Competitive threat Post Office faces both opportunities for and threats to income from our competitive market place. - The Mails and parcels market remains intensely competitive. - Use of digital channels affecting customer journeys, new products and back office functions is changing propositions and customer expectations. - Financial Services is a challenging market with new entrants such as challenger banks and Fintechs.. Responding quickly to different strategies, business models, and products is therefore essential to growth.	Crystallisation of these risks could result in not achieving our growth objectives, losing market share and revenues.	• Customer perceptions and competitor behaviour are key inputs to decision making. • Our strategy focuses on customer requirements, market trends and competitor behaviour, working with partners where appropriate, to offer customer centric propositions, supported by a clear distribution strategy. • Each product proposition developed in the context of a customer strategy which describes target market, channel of distribution and completing attributes.
Dependency on strategic relationships Post Office has strategic relationships which are key to its product offering and growth, for instance with Royal Mail Group and Bank of Ireland (UK) plc. Misalignment of the strategic direction or focus with the strategic partner could result in products that do not support our growth strategy or meet our customer or market requirements.	This could result in not achieving our growth objectives, losing revenue and market share.	• Close working relationships established with our strategic relationships. • Interactions scheduled with our strategic partners to improve the product offering and service to drive growth and profitability for both parties. • Contractual arrangements monitored and managed to ensure that they are aligned with commercial objectives and that relationships deliver to expectations.
OPERATIONAL AND FINANCIAL RISKS		
Lack of appropriate capability The Post Office is dependent on its dedicated work force to meet the expectations of its customers and stakeholders. Continuing to attract, motivate, develop and retain people is key to its success.	This could result in not achieving our strategic objectives and loss of staff engagement.	• Continual review of our organisational structure to ensure it evolves and supports our requirements. • Key capabilities for our current and future state needs identified with a capability heatmap. • Investment in developing our people.
Decline in customer experience If we are unable to deliver an attractive customer experience, via our products, service and channels, we risk losing the support of our customers.	This could result in reduced customer satisfaction and brand reputation, with consequential loss of market share and revenues.	• Customer strategy continually monitored to ensure that it meets changing customer product and service expectations and reflects current market and competitor trends. • Channel strategy ensures we meet the changing customer requirements for access and utilises available and emerging technology to reflect changing customer needs.
Unattractive network proposition As we transform, there is a risk that the Post Office may not be able to retain, or attract sufficient new, retail partners because of the complexity of our	As well as loss of revenue, this could result in shrinkage to our network and breach	• New branch model being developed to provide retailers with an attractive proposition relative to other categories. • New branch model also ensures that we use modern technology to drive simplicity of operations,

Post Office ARA 2016/17, draft risk section for RCC

POL00401624

network proposition and relative value to the retail partner particularly compared to other categories.	our public purpose commitment.	efficiency and cost reduction for the retailer, as well as a better customer experience. • Branch model continually reviewed and updated to respond to ongoing competitive threat and market conditions.
Business interruption and cyber threat Post Office is dependent on the continued availability of its information systems and associated infrastructure. These could be threatened, either due to internal issues, external events or cyber attack.	This could result in disruption of service leading to negative customer experience, breach of contractual obligations and brand damage.	• Business continuity plans updated through review, testing and enhancements. • New contracts have provisions covering the security, resilience and availability of our IT systems and infrastructure. • Information Security policies in place. • Penetration testing schedule to assess and improve the security of our systems.
IT and Change complexity The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity.	This could significantly impact PO strategic objectives and execution and implementation of PO business strategy.	• Appropriate Governance structure for Change Delivery. • Integrated Master Plan to manage and monitor progress across the portfolio including dependencies. • A single view of all Change to avoid complexity across the Change portfolio. • Early identification and engagement of stakeholders to ensure appropriate planning.
Stakeholder funding The cost of delivering the public purpose of the Post Office and meet the expectations of stakeholders may exceed current forecasts.	This could result in not achieving our growth objectives, failing to meet our public purpose commitment and damaging our reputation with stakeholders.	• Proactive engagement with stakeholders to ensure there is full understanding of, and alignment with, the strategic goals and the investment case required to deliver them. • Annual and three-year operating and capital plans developed and risk assessed. • Scheduled feedback to stakeholders and review.
Financial reporting and controls failure Our financial controls are fundamental to delivering our fiduciary responsibilities, management information, financial reporting and compliance with accounting and governance standards. These may not operate effectively if they are not documented, reviewed and monitored regularly.	This could result in loss of revenue, increased costs, financial misstatement and damage to reputation with stakeholders.	• Defined and structured delegation of authority which is reviewed and approved by the Board. • A Financial and Accounting manual and a framework of supporting general controls – see our General Controls Framework on page XXX. • Documented financial controls, with additional assurance to be provided from a Control Self-Assessment process.
LEGAL & REGULATORY RISKS		
Financial regulatory breach The Post Office operates under an extensive regulatory environment, covering areas such as financial and postal services, telecoms, procurement, competition law and data security. This environment continues to evolve, particularly in the financial services arena, and we need to ensure that the changing requirements continue to be identified and met.	This could result in regulatory censure, fines, litigation or curtailment of trading, which could impact income and/ or damage our reputation with customers and suppliers.	• New regulatory obligations monitored by relevant business owners, with support from Corporate Services. • On-going training to our staff on legal and regulatory matters. • Regular compliance tests and monitoring are conducted. • Internal and external assurance programmes are in place (including by our regulatory principals) to ensure that we meet financial services regulatory requirements, including sales practices and conduct, customer experience and product experience and delivery.

POL00401624

4.1) Supply Chain Pilot of the Placemat

Author: Richard Williams/Deana Herley Sponsor: Jane MacLeod Meeting date: 4 May 2017

Executive Summary

Context

In January 2017 the RCC agreed that the placemat methodology would be piloted in Supply Chain, and it was agreed that the results of the pilot would be brought back to the May RCC meeting ahead of the May ARC. Since then the central risk team have worked with senior Supply Chain management to develop and roll out the underlying methodology that would enable assessment of those risks relevant to Supply Chain. This paper summarises the initial results of the pilot.

Questions this paper addresses

- What have we learnt?
- How has the pilot been implemented?
- How is it scalable and where next?

Conclusion

1. During the pilot the central risk team developed a suite of tools to enable local management to assess the level of risk relevant to each business area and the effectiveness of the control framework. The initial results for Supply Chain are being reviewed; and will be released as part of a wider review of Finance and Operations. As the placemat methodology is rolled out more widely, it will be possible to establish more objective comparative risk assessments.

2. A suite of tools and the accompanying methodology has now been developed and this will facilitate the roll out across the business. The assessment of risks and controls is undertaken through workshops with the relevant line managers. In the case of the Supply Chain pilot, this enabled management to better understand the risks affecting their particular areas of responsibilities, assess the effectiveness of the various controls, and ensure a greater awareness of areas where risks could be outside perceived appetite.

3. The pilot in Supply Chain required approximately 20-25 man days of work from the central risk team, and a number of risk workshops attended by line management. This

POL00401624

included a one off exercise to produce the documentation setting which set out the minimum standards for the business, templates, workshops etc.

4. Following discussions with the CFOO it is proposed that the process now be applied to the other areas within Finance & Operations with a view to these being completed in time for reporting to the September RCC and ARC.

Input Sought

5. The Committee is asked to review this report and confirm its support for the direction of the roll out of the Placemat approach.

The Report

What have we learnt?

6. Implementation of the Placemat in each business area will enable management to:
   - identify the top risks which may prevent strategic outcomes;
   - embed a risk framework which is aligned to business strategy;
   - achieve a consistent application of minimum standards;
   - enhance the risk culture and risk ownership at all levels and improve our ability to identify, understand and proactively respond to risks in a prioritised way;
   - improve the understanding and identification of cross functional risks and dependencies;
   - link capabilities, key processes, risks, controls and assurance activities which help to understand the impact of future change;
   - inform the Internal Audit planning process and over time refocus activity on the effectiveness of governance and assurance arrangements; and
   - develop appropriate and proportionate framework for continuous reporting of risks with the opportunity for pragmatic challenge at RCC, ARC and Board.

7. As part of the process, 'business area leads' in conjunction with their lead teams and Risk Champions were requested to rate each principle risk; and identify those which were not applicable, or where reliance was placed on the controls operated by a different business area. This process demonstrated the dependencies, and helped to assess the adequacy of existing controls and the need for any remediation or additional controls.

8. The risk rating process takes into account:

Likelihood and impact of risks
Effectiveness of design and operation for controls (self-assessment)
Minimum standards by principle risk
Reported risk incidents and exception requests
Internal and external assurance, including audit findings and follow up

9. Once the initial review is completed each business area will review the Placemat at regular intervals (quarterly) through risk discussions to provide a continuous pulse of the business risk and control environment.

POL00401624

10. The principal risks will also need to be reviewed periodically to ensure that the Placemat continues to assess and report on the risks that the business considers to be most significant.

How has the pilot been implemented?

11. We presented proposed principal risks to the RCC back in January 2017. Subject Matter Experts (SME) were subsequently identified and, with their assistance, the Central Risk Team developed a suite of documentation, which describe the expected governance, risk management and control arrangements as well as minimum standards and key risk indicators, where they currently exist.
12. As a starting point the Supply Chain capabilities listed within the Target Operating Model (TOM) were re-agreed with management to help identify risk and controls associated with the key enabling processes to those capabilities.
13. The outputs of this exercise informed which principal risk categories of the Placemat were applicable or where reliance was placed on controls operated by another area. A series of follow up sessions were held with key personnel to establish an understanding of those key processes, risks, controls and assurance in greater detail. The design and operation of a sample of controls were also tested.
14. As an initial output of the pilot, the Risk Register for Supply Chain has been reviewed and updated to better reflect risks to capabilities and Placemat principal risks. As a second output a 'Risk and Control Matrix' (RACM) has been developed which describes existing controls. This process enables risks to be prioritised and ensures that remediation proposals are pragmatic.
15. As a final step the Placemat will be populated by assessing and rating each principle risk based on a combination of: risk *scoring, existing controls, sample testing, minimum standards, incidents, exceptions and assurance.* In addition, any assurance activity can be mapped to risks and controls.
16. Although risk ratings are subjective, greater consistency will be achieved by reference to the harm table and development of minimum standards.
17. Once the placemat is populated an overview can be obtained of those risks which must be remediated. Further work is underway in Supply Chain to develop this view.
18. Completion of the Placemat will then allow the development of the following:
    a. an integrated risk management information pack to support discussion at lead team meeting, including key risks, control effectiveness, assurance activity and risk incidents and losses.
    b. Key Risk Indicators (KRIs) and risk scenario testing, to further enhance management of risk.
    c. On-going support mechanism for review and re-assessment.

POL00401624

How is it scalable and where next?

19. The approach taken to implement the pilot was designed for wider roll out. For example the documentation that sets out the minimum standards for the business, templates, workshops etc.
20. Approximately, 15 man days have been spent by the Central Risk Team in developing the supporting documentation, as well as additional time spent preparing for and conducting workshops. More complex business areas will necessarily require more time, although the templates for the supporting documentation now exist. Roll out will require the support and cooperation from key personnel within each business area, and resource within the Central Risk and Assurance teams.
21. Following completion of the initial Placemat assessment by each business area, regular reviews can be undertaken by the relevant Risk Champion, as well as more formal re-assessment of Placemat ratings at agreed intervals to ensure it remains current.
22. We have been asked by the CFOO to replicate the scalable approach with colleagues from wider Finance and Operations teams to give us the ability to assess a consolidated / holistic view of key risks proportionately, understand the interdependencies and prioritise any remediation activity.

Conclusion

23. The Placemat approach, and development of the supporting documents, tools and outputs has supported Supply Chain management to create a central view of its key risks which can therefore be prioritised (based on controls and assurance activity). We propose that Supply Chain undertakes a reassessment of Placemat in September.

POL00401624

4.2) Business Continuity & Crisis Management update

Author: Tim Armit Sponsor: Jane MacLeod Meeting date: 4th May 2017

Executive Summary

Context

Implementing pragmatic strategic recovery capabilities and identifying impacts continues across all sites. Swindon has been assessed and strategies for recovering key assets is being undertaken. Chesterfield is planning a full day exercise at the recovery site. Industrial Action planning is being facilitated through a workshop to assess the impact of a Royal Mail strike.

Questions this paper addresses

1. What is the current business continuity status?
2. What are the next steps?

Input Sought

The Committee is requested to note the report.

POL00401624

Conclusion

- Chesterfield Recovery Site Full Day Test

The capability to operate at the Sungard Leicester Recovery site has been proven. The next step is to now take a cross section of key areas from Chesterfield to work for a full day at the recovery site. How this is to be done and who is involved is now being planned. The exercise is aimed for the end of June 2017.

- Swindon Review

A visit to Swindon has been undertaken and an assessment of the options for recovery are being considered. What is key to Post Office and Royal Mail is being analysed and strategies to recovery key operations at an alternative Supply Chain Depot are being reviewed. Options will be discussed with Supply Chain management for agreement in June 2017.

- Royal Mail Industrial Action planning

There is a real risk that Royal Mail may strike later in 2017. A workshop is being facilitated in the next few weeks to bring together all operational areas which might touch Royal Mail operations in any way. The objective of this is to assess the impact on Post Office operations of Royal Mail being down. Then to consider what options are open to Post Office operations to mitigate any impacts which would become intolerable.

POL00401624

5.1) IT Controls Update

Author: Sharon Gilkes | Sponsor: Rob Houghton | Meeting date: 04 May 2017

Executive Summary

Context

In response to the Deloitte findings from September 2016, the Post Office took a decision to implement a sustainable IT Control Framework (ITCF). This will help ensure that there is more confidence in IT operations to mitigate risks in areas such as security breaches, unreliable data integrity, or loss of service. This will bring the Post Office IT controls more in line with good industry practice.

We are implementing ISACA's Control Objectives for IT (COBIT5) as the framework that maps IT operation processes and risks, identifies remediating controls and introduces evidenced self-assessment and monitoring. The purpose of this paper is to update the ARC on the implementation progress made and the priorities for FY2017/18.

Questions addressed in this paper

1. What progress has been made in implementing the IT Control Framework?
2. What are the next steps and when do we expect to complete the work?
3. What addition control improvements are planned or in progress?

Conclusion

To date over 100 control gaps have been identified. Of these 9 have been rated as high risk. We have defined 16 remediation plans and are validating these with the suppliers.

We knew that our IT operating models for the majority of our IT suppliers are different and not aligned (highlighted in IT strategy). This work has further evidenced the delivery and control issues this gives rise to.

The work has also reinforced a theme which underlines many of our IT service delivery issues. The IT eco-systems (IT operating models) for PO and the majority of our IT suppliers are different and not aligned. This work on the creation of the ITCF has further evidenced the delivery and control issues this gives rise to. This is covered in more detail in section 6 below.

The plan has been adjusted as we have moved into detailed planning with our suppliers – there is no cost impact as a result of this but the timeline moves to the right on certain outcomes. The development of the ITCF based on COBIT5 is on track overall, and the planning adjustments reflected in our updated project timeline (section 7).

POL00401624

Input Sought

The ARC is asked to note the progress made and comment on the priorities and approach.

POL00401624

The Report

Introduction

IT service delivery relies on over 90 suppliers, some of these suppliers operate under contracts drawn up many years ago which we have inherited within the Group CIO function. We therefore need to ensure active cooperation and support of the third party suppliers which makes the project significantly more complex and therefore more resource intensive.

KPMG are assisting us with identifying the key issues in our ITCF and maturity gaps, and are working with our teams and IT suppliers to improve the ITCF and enhance the IT operating model.

It should also be noted that the improvement programme requires the support of the suppliers and that current contractual obligations upon the suppliers to cooperate do not exist in many cases. Therefore this is a challenging task, as many of these suppliers support our critical IT systems and services. We also need to ensure that improvements minimise the impact on the suppliers' delivery of existing IT service levels to us.

What progress has been made in implementing the IT Control Framework?

Item	Description	Status (As at 26/04/17)
Process Mapping	1) End to end process mapping is being conducted in the form of 'walk throughs'. This will identify controls and create a permanent record of how we work. 2) Each process will have an accountable person and identified responsibles.	Complete
Risk and Control Matrices (RACMs)	Controls will be identified (with owners) to mitigate risks in our business operations. These risks and controls will link logically and directly into the Post Office's higher level (group) risks to ensure a clear "line of sight" from individual controls to Board-level risks. (see diagram below). This will ensure sufficient and appropriate controls are implemented to address the Post Office's business risks.	This activity is now in progress with reviews for 9 out of 11 process areas already underway.

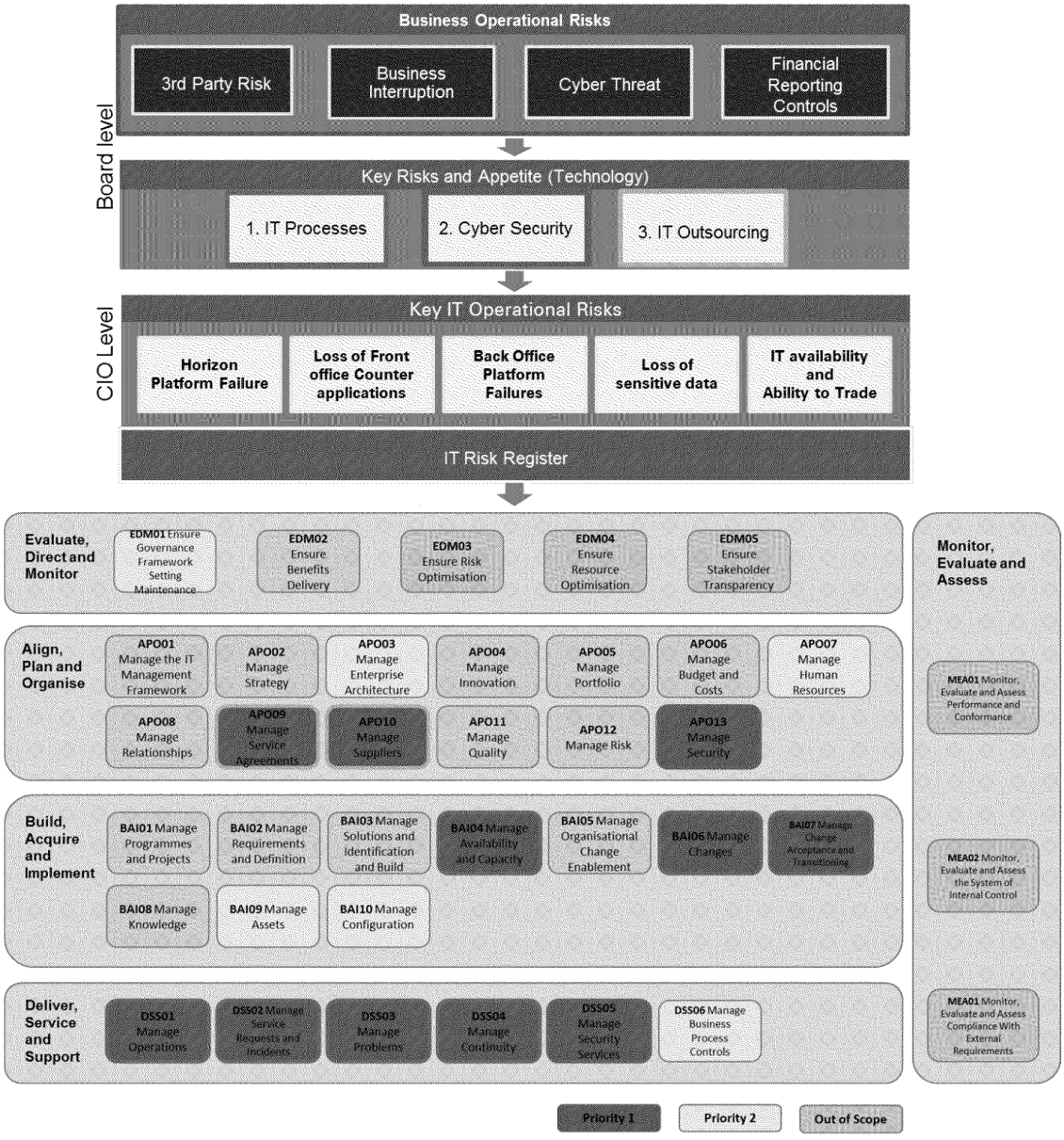
POL00401624

Gap identification	The process walkthroughs and results recorded in the RACMs will identify where controls are absent, badly designed or inadequate.	Following interviews with PO process owners, we have already identified gaps for 6 out of 11 processes. We are engaging with suppliers to complete the walkthroughs and validate gaps.
Gap remediation	Remedial steps will also be agreed with control owners and recorded in the RACMs for ensuing progress tracking, evaluation and reporting via the TrAction tool.	We have set out suggested remedial actions for 3 out of 11 processes, having linked them to existing improvement plans, where possible.
Self-assessment	Control owners confirm, using established software, and evidence that their control was operating effectively in the previous period. Process Owners will be requested to complete a quarterly checklist to ensure responsibilities are being carried out as well as, identifying any exceptions.	To commence upon completion of Gap remediation. Planned circa June 2017.
Assurance	Internal Audit will perform independent sample testing of KPMG outputs, Self-Assessment and control evidence.	To commence upon completion of Gap remediation. Planned circa June 2017.

1. The diagram below shows how we have ensured that controls examined and recorded in the RACMs link logically and directly into the Post Office's higher level (Group) risks to ensure a clear "line of sight" from individual controls to Board-level risks.

2. The highlighted areas of the COBIT5 framework (dark green) are currently included in this review; with the light green areas being implemented in the second stage of the project. The grey process areas are not being implemented as they are not critical control areas to address the business operational risks.

POL00401624



3. We have established process owners for each of the Priority 1 areas above and they are updating to risk register on a monthly basis and continuously monitored. Walkthroughs are underway for 9 out of the 11 processes in-scope and those are progressing well. To date over 100 gaps have been identified of varying severity. Note this is emerging work and needs further analysis.

POL00401624

4. To allow easy transfer of our findings into TrAction (PO's self-assessment monitoring tool), we have aligned our documentation (for the ITCF) to the format used for Financial Control Framework recording.

5. The key critical control failures identified so far and what we're doing about them:
    a. The operational Change Management process seems to work for suppliers who have been on-boarded within the SIAM tower structure. However, some of the suppliers who are outside the tower model (e.g. Royal Mail group, Clients Banks, DVLA (although they have recently been on-boarded), etc.) sometimes do not supply their change information via the IT change advisory board (CAB) process. This inconsistency can cause change conflicts. To address this, we have appointed an interim IT Change Manager (and are in the process of recruiting an IT Change and Release Manager) to improve adherence and governance around all types of change.
    b. System Data Edits/Reference Data updates are not governed by the CAB process, and the existing process (currently managed by Atos) has encountered some issues recently. This issue is now being investigated with the aim of getting data edits/reference data changes to comply with the change categorisation and governance model.
    c. PO does not have a way to correlate current Firewall changes with a business justification. Firewall rules govern all external/internal access to PO and are, therefore, critical. This includes Firewalls managed by Fujitsu, Verizon, Computacenter, CSC, Accenture, 3M and Atos. There is no clear mapping for Firewall rules to indicate which critical services are affected by them. We have an initiative to address Firewall rule governance under the SOC program which is currently in progress and expected to be delivered by circa September 2017.
    d. Following a review of severity 1 and Severity 2 incidents, it has been identified that an average of 50% of incidents are resolved outside of the SLA for resolution. We are addressing this by updating our Critical Service list which will be shared with the Atos Service Desk and Incident management this will ensure that the incidents are assigned to the correct resolver group and prioritised correctly.
    e. There is a register which captures "known errors", however, it is not being utilised. This means that there are no controls in place to minimise service outages from reoccurring. The "Known Errors" report will be reviewed on a monthly basis, including trend analysis of recurring problems

6. The table below provides a summary update for 6 out of the 11 processes in scope, where gaps have been identified already. The priority assessment (HML) is the current state and may change as we continue to validate gaps with IT suppliers.

POL00401624

RACM	No. Cntrls	No. Gaps	H	M	L	Example of high priority gaps	Exemplar Remedial Actions
1. Manage Changes	7	16	1	9	6	• All changes to operational environment are required to go through CAB. However, this is not consistent across all suppliers, which has resulted in operational incidents occuring. • When changes are put through and fail, they are supposed to produce a Post-implementation review (PIR), however PIR's are often not shared with PO.	• Review / improvements to be made under Target Operating Model (TOM) • Formal sharing of PIR's is to be agreed with ATOS
2. Manage Service Requests and Incidents	9	24	3	13	8	• All service requests and incidents should be managed via the IT Service desk provided by Atos. However, some suppliers have not been integrated within this framework and service incidents with these suppliers are carried out on a reasonable endeavours basis by Atos.	• Being addressed as part of the strategic service desk review work. • For Services identified as critical, this will be direcly addressed under that Improvement plan. For non-critical services this will be addressed following completion of tasks associated with Critical Services • To be addressed under Review/improvements to be made under Target Operating Model (TOM)
3. Manage Problems	6	13	2	6	5	• Problems are actioned and then closed by ATOS without PO's knowledge or briefing. Once a call is logged there is no visibility for PO as to how it is dealt with. • The problem management process needs to be further improved as ATOS do not review problems from suppliers out with their tower arrangement.	• This is now picked up in the monthly problem review and is being addressed and continously monitored • Being addressed as part of the strategic service desk review work. • This will change with the IT TOM work. It is envisaged that an ATOS service manager will be dedicated to each Head of IT. ATOS has also been asked to include recurring problems across supplier in the monthly pack.
4. Manage Security	3	4	4	0	0	• There is a limited Information Security Management System (ISMS) in place.	• A Security Transformation Programme has been put in place and a revamped IT Security Function has been stood up to provide more proactive IT Security Operations. This will include the setting up of a Security

POL00401624

							Operations Centre (SOC).
5. Manage Security Services	7	34	3	8	23	• No awareness of encryption and post-intrusion protection on PO desktops and no visibility over protection implemented on personal devices connected to the PO network. • PO IT has no comprehensive IT asset inventory. • It is unclear where all personal, commerically or legally sensitive/privileged data is being held. • No current capacity to gather and analyse logs of security related events. • Although ATOS provide an overall aggregate service, there are gaps in the arrangement with suppliers outside their arrangements, and the management of IT from current vendors is not proactively actioned.	• A Security Transformation Programme has been put in place and a revamped IT Security Function has been put stood up to provide more proactive IT Security Operations. This will include the setting up of a Security Operations Centre (SOC).
6. Manage Change and Acceptance Testing	10	13	0	9	4	• No common checklist used by project managers to reference to instruct them on the required steps for implementation plans. The 'One Best Way' pack is not easily available and regularly used by PO PMs. • Lack of visibility over planing and resourcing for testing as this is primarily handled by ATOS. Lack of clarity on whether test plans identify necessary resources to execute testing and evaluate results. • Lack of a standard PO process for post-implementation review involving the Project Manager. • There have been examples where Change Acceptance and transition to live has not been as rigorous as needed (e.g. Credence service novation to Accenture)	• All projects now have a Service Design and Acceptance plan built in to capture non-functional requirements. Also the Heads of IT Service will now be accountable for all changes being passed into the Operational domain.
7. Manage Service Agreements	5	Planned for w/c April 24th					
8. Manage Suppliers	5						
9. Manage Availability and Capacity	6						
10. Manage Continuity	Planned for w/c May 8th						
11. Manage Operations							
Total to date	**58**	**105**	**9**	**45**	**50**		

What are the next steps and when do we expect to complete the work?

7. We are on track with interviews for the Priority1 processes, although due to the nature of the Atos role in managing controls through to the rest of the IT eco-

POL00401624

system, the process of identifying the control gaps with suppliers is taking longer than planned.

8. We have re-issued an updated Terms of Reference to all in-scope IT suppliers to address this, and have active engagement with their relevant Exec Sponsor.

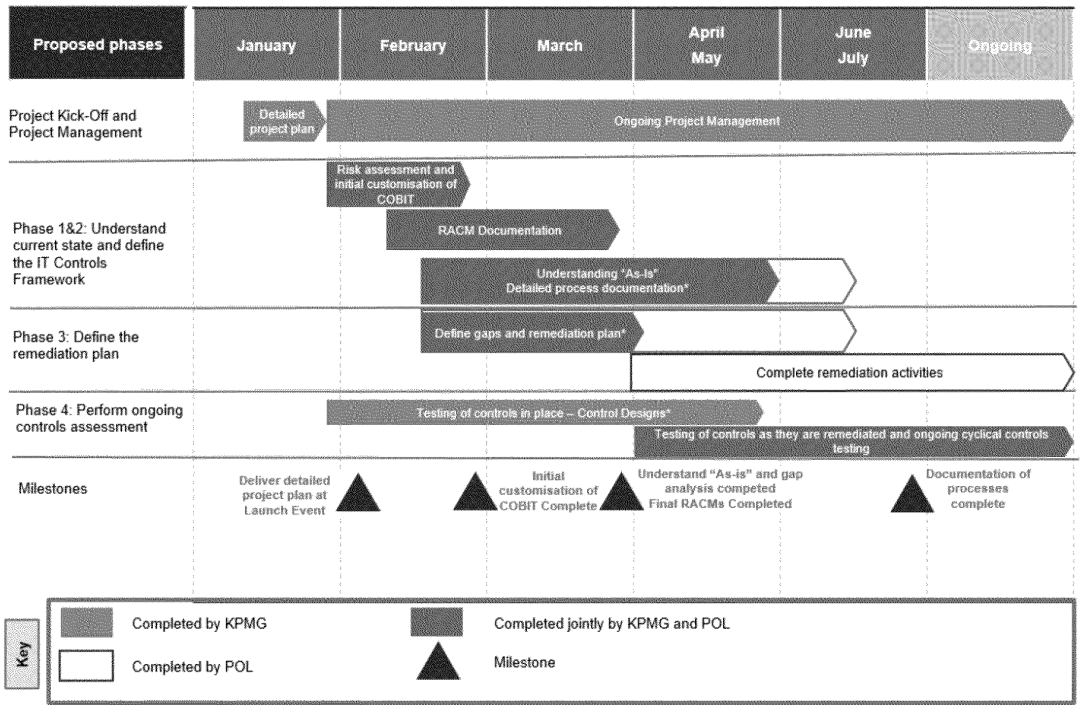
9. Formal updates on ITCF progress are now a standing agenda item on the CIO IT Operations Board, and are monitored and tracked through the IT Risk Register.

10. Further IT Supplier walkthroughs are planned for the coming weeks as we progress with the gaps identification effort.

11. We are providing the wider IT team with access to the PO control framework self-assessment tool (TrAction).

12. Remediation plans will continue to be agreed with PO nominated process owners and walkthrough sessions will continue with our IT suppliers to validate the findings.

13. The timeline below depicts the key activities and the order in which they are expected to occur.



* Includes walkthroughs with relevant suppliers

POL00401624

What other control improvements are planned or in progress?

14. As noted in the update presented to the ARC in March, we are undertaking a systematic review of the way we manage critical IT services through Atos, and are developing a proposed new IT operating model which would require ongoing discussions and re-negotiation with our other IT suppliers.
15. It was also noted that PO's outsourced IT operating model would require new and legacy IT suppliers to be part of the ITCF self-assessment, we will be embedding this at contract renewal/on-boarding stage.
16. Internal Audit are supporting the ITCF project to ensure the appropriate embedding of IT controls, which will provide transparency and addition assurances over alignment with operational risks.
17. Working with EY, we will aim to improve the quality and ease of the audit of IT controls, and in Q3 assess whether and to what extent we need to review the additional testing performed for the 2016-17 audit.
18. Following an Internal Audit review of IAM/JML process (identity access management/joiners-movers-leavers), a PO cross-functional working group has been created to address identified gaps in the current processes and progress a remediation plan.

POL00401624

Financial Reporting Controls

Author: Danielle Goddard Sponsor: Amanda Radford, Al Cameron Date: 4 May 2017

Executive Summary

Context

The purpose of this paper is to update the RCC on the status of the Financial Reporting Controls Framework (the FRC) and the assurance that can be taken as at the financial year end, as well as the next steps into the second phase of the project.

Questions addressed in this report

1. What is the status of the FRC and what reliance can be taken as at year end?
2. What progress has been made since March and what further work will be undertaken?
3. What are the next steps into the second phase of the project?

Conclusions

At the financial year end there were 241 controls identified for reliance. Of these 241, 171 (71%) were issued for self-assessment at the end of March. 168 (99% of those issued for self-assessment) were self-assessed as operating effectively. The remaining 3 were not self-assessed but have been discussed with the control owners and confirmed as operating effectively for the period.

Of the 70 controls not issued for self-assessment 19 were not due to be operated in the period, 19 were automated controls which are being sample tested centrally, 18 controls were in remediation at year end, 11 controls were still being set to live, and 3 were pending confirmation of ownership.

All 18 controls still in remediation at year end have been reviewed and work-around controls have been performed or testing procedures are in progress to gain comfort for year end. The 11 controls being made live for self-assessment relate to the overall control environment and are under review to ensure there are no unaddressed risks at year end.

PwC have now tested 59 controls over 10 of the 12 processes; 48 operated effectively, 11 had exceptions but were classified as minor. PwC are currently completing their testing over the remaining 2 processes and annual controls; this is expected to be complete in early May.

We no longer consider any of the original 10 high risks gaps to be high risk. 3 remain open as medium risk with workaround controls in place, the remaining 7 are closed and the remediated controls are operating as BAU.

POL00401624

Areas that have been added to the scope of the FRC in recent months are advancing. We are documenting Masterdata controls and beginning to agree remediation plans for identified gaps. The four other areas added recently, of lower risk, are underway. We are re-assessing controls over fixed assets, given the potential change in accounting estimate and reversal of impairment. A business review is underway over the purchase to pay process.

Input Sought

The RCC is asked to note the progress made and comment on the priorities.

The Report

What is the status of the FRC and what reliance can be taken as at year end?

1. Across the FRC, we are seeking to rely on 241 controls. Of the 241, 168 were self-assessed in March. 18 controls were still in remediation, 11 were still due to go live, and 3 were live but not submitted (although discussions with control owners have confirmed that these were operating effectively). 19 were not due for self-assessment in the period due to operational frequency, and 19 were automated controls which are being sample tested centrally.

March 2017 - Total controls	**241**	
Less: Controls in remediation	-18	
Controls to be assigned	-3	
Controls to be set to live	-11	
Controls not due to be operated due to frequency	-19	
Automated controls subject to central testing	-19	
Total population for self-assessment	**171**	**71%**
Self-assessed and operated effectively	168	98%
Self-assessed but not operated effectively	0	0%
No self-assessment submitted	3	2%

2. 98% (168 controls) were self-assessed as operating effectively: the other 3 were not self-assessed. Conversations have been held with control owners to understand the reason for the 3 not submitted, however all have been confirmed as having been operated during the period. See appendix 2 for further detail of March CSA results by process.

3. PwC has now undertaken a further phase of independent sample testing. A total of 59 controls has now been tested across 10 processes with a population of 217 controls (27% sampled). 11 controls need some improvement: these are mostly

POL00401624

re-wording of controls or ownership issues which have since been resolved. See Appendix 1 for testing results by process.

4. We had 10 high risk gaps in the initial assessment. At end March, no high risk gaps remain. 3 medium risk gaps remain but had work-around controls in place providing assurance at year-end.

Gap	March ARC	May ARC	Comment
Period end checklist	Closed	Closed	Operating on a monthly basis; period end is not closed without completion of checklist or mitigating checks.
Journal authorisation	Closed	Closed	Operating on a monthly basis. All CFS journals over £250k P&L or £1m Balance Sheet impact receive independent authorisation from an agreed approver before being processed by a central independent team.
Balance sheet review	Medium	Closed	Monthly FLT Balance Sheet review now in place.
Independent b/s review	Closed	Closed	Operating on a monthly basis; Balance Sheet probity requires independent review before submission to the Central team.
Branch cash reconciliation	Medium	Medium	Reconciliations are now in place for branch sterling and bureau cash between Horizon and POLSAP. System reports are being developed with Fujitsu for cash in transit, where stronger workaround controls exist.
Review of good receipting	Medium	Closed	Operating on a monthly basis with strong return rate.
Payroll segregation	Medium	Medium	Effective workaround controls in place through independent reviews until Success Factors goes live.
Quality of bank recs	Closed	Closed	Operating on a monthly basis. Improvement noted by external audit team.
Quality of b/s recs	Medium	Medium	Reviews and training underway but continuing into new financial year; central review performed for year end.
Spreadsheet controls	High	Closed	Remediation completed for all spreadsheets. PwC are currently testing.

POL00401624

What progress has been made since March and what further work will be undertaken?

5. Since the March RCC we have reduced control gaps from 24 gaps to 18 gaps. We have performed review procedures and implemented work-around controls to ensure that we had adequate assurance at year end.

6. We have also made a further 12 controls available for self-assessment by setting Control Environment controls live for self-assessment. A further 11 controls still remain which require setting live for the April self-assessment.

7. PwC testing has continued and a further 17 (total 59) controls were tested with 3 (total 11) exceptions being identified. We do not assess any of these exceptions to be high risk however these have all been addressed or are in progress. PwC are performing their final phase of testing and we expect to see results in May; this will include testing of the remaining 2 processes and annual controls. PwC will test high risk controls e.g. Spreadsheet controls.

8. We are re-assessing controls across Fixed Assets. The financial reporting risk has changed within fixed assets due to the potential change of impairment and for this reason we are re-assessing risks and controls in this area.

9. We are also reviewing ownership of controls as part of the new roles and responsibilities in the finance restructure.

What are the next steps into the second phase of the project?

10. We added Masterdata to the scope of the FCR in Q3. Documentation of processes, risks and controls has been completed across 2 of the 12 relevant data sets (Vendor and Customer), with approx. 30 controls being identified and 8 control gaps (excluding duplicate controls across the 2 processes). Most of the gaps are due to reliance on manual processes with a lack of monitoring controls. None of the gaps indicate a risk of material misstatement however are currently in the process of being prioritised as high, medium or low risk.

11. Documentation of risks and controls is already underway for a further 2 Masterdata sets (GL and Payroll); these will be completed in May 2017.This will then be extended to cover the remaining in scope data sets; Project Accounting, Fixed Assets, Bank & Cash, Product, Branch, Stock, Tax and Internal Orders. We expect these to be completed by end August 2017. Controls will be loaded for self-assessment and a remediation plan developed for gaps. Additional checks are in progress to ensure no implications for the financial statements; no implications have been noted so far.

POL00401624

12. A site visit has been scheduled for early May to review Masterdata controls operated by Atos, to assess the control environment and any gaps which require remediation.

13. As noted previously, in reviewing the programme we have identified a further four areas that we want to add to FCR which were not considered high risk and were not in the original scope: agents' debt; the branch correction process; agent remuneration; and POMs. A business case is being submitted to cover this, as well as; the remaining Masterdata work to be performed, Finance Service Centre controls, and Cash Management and Forecasting controls.

14. The Director of Procurement is leading an end-to-end review of the purchase to pay process across our business. End to end processes are currently being documented, and the team are assessing what can be remediated now as well as working up alternatives to our SAP solution. In tandem Finance are recasting all the cost centres and project codes for the business and realigning them with the new business structure so a significant amount of work is going into seeing where we can improve our manual controls and generate some automated reporting to assist with this. The output will be a business case in the coming months, which is likely to form part of the Back Office project.

Appendix 1 – PwC independent assurance results

Testing phase	Process	Total controls in process	Controls tested		Exceptions identified		Red Exception	Amber Exception	Control operating effectively	
Phase 1	Client Settlements	14	7	50%	0	0%	0	0	7	100%
Phase 2	Project Accounting	11	2	18%	1	50%	0	1	1	50%
Phase 2	Record to Report	38	12	32%	2	17%	0	2	10	83%
Phase 2	Tax	16	4	25%	0	0%	0	0	4	100%
Phase 2	Fixed Assets	19	5	26%	3	60%	0	3	2	40%
Phase 2	Payroll	35	10	29%	2	20%	0	2	8	80%
Phase 3	Bank and Cash	27	7	26%	1	14%	0	1	6	86%
Phase 3	Bill to Cash	18	3	17%	1	33%	0	1	2	67%
Phase 3	Treasury	14	4	29%	0	0%	0	0	4	100%
Phase 3	Procure to Pay	25	5	20%	1	20%	0	1	4	80%
		217	**59**	**27%**	**11**	**19%**	**0**	**11**	**48**	**81%**

There have been no 'red' (high risk) exceptions identified. 2 red exceptions were identified initially however evidence was subsequently provided to PwC which meant that these exceptions were later re-evaluated as 'amber' (low risk).

11 amber exceptions have been identified, mainly relating to ownership issues, and wording changes. These have since been resolved.

POL00401624

Appendix 2 – March CSA results by process

Total Controls	Control Gaps					Control Owners		March CSA Results				
Process	Total Controls	Control Gaps	H/M/L Impact of H	M	L	Owner Assigned	No owner assigned	Controls operated effectively	No self assessment submitted	Not operated due to agreed frequency	Self assessment submitted but control not operated	Controls to be set to live
Bank & Cash Management	33	2	0	2	0	32	1	28	0	2	0	0
Bill To Cash	17	3	0	2	1	17	0	12	0	2	0	0
Control Environment	21	1	0	1	0	21	0	8	0	1	0	11
Fixed Assets	18	3	0	0	3	18	0	14	0	1	0	0
Payroll	34	1	0	1	0	34	0	29	0	4	0	0
Procure To Pay	24	1	0	1	0	24	0	12	1	10	0	0
Project Accounting	9	2	0	2	0	9	0	3	2	2	0	0
Record To Report	38	3	0	3	0	38	0	30	0	5	0	0
Settlement Process	14	0	0	0	0	12	2	12	0	0	0	0
Stock	7	2	0	1	1	7	0	5	0	0	0	0
Tax	16	0	0	0	0	16	0	7	0	9	0	0
Treasury	10	0	0	0	0	10	0	8	0	2	0	0
	241	**18**	**0**	**13**	**5**	**238**	**3**	**168**	**3**	**38**	**0**	**11**

POL00401624

5.3 Financial Crime Risk Update

Author: Sally Smith Sponsor: Jane MacLeod Meeting date: 4th May 2017

Executive Summary

Context

This paper updates the Risk and Compliance Committee on progress with the HMRC Regulatory Activity project which has been established to manage both the HMRC's Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) audit and the risk assessment work being undertaken to address Financial Crime Risks.

Questions this paper addresses

- What is the current position on the HMRC Audit and potential Branch Registration Penalty?
- What is the current position on progress with the Financial Crime risk assessment work and next steps?
- What are the impacts for Post Office of upcoming regulatory changes

Conclusion

1. HMRC met with us on 22nd March to issue their audit findings, including regulatory breaches which are currently under consideration by them for sanctions. Their findings are broadly in line with those already identified through our risk assessment work, and a further meeting was held with HMRC on 5th April to review the action plan already in place, the work being undertaken on Bureau de Change and enable Post Office to seek clarification and guidance. The next meeting is being held on 16th May with a view to agreeing a robust action plan and milestones with HMRC, and further regular meetings will be held through the year, with HMRC planning a review of Bill Payments later in 2017.
2. HMRC have advised that the penalty for historic branch premises registration errors will be c. £785k, although to date the pre–penalty notice has not been received. HMRC also advised there will be no changes to the annual registration processes for Post Office this year.
3. Further risk assessments are broadly on plan, with work on Drop & Go nearing completion and good progress being made on MoneyGram and Giftcards. Risk Assessment work for POMS and their insurance products was prioritised for April and is due to be completed in May. A project team and steering group have been established to address the control weaknesses identified in the Bureau de Change risk assessment and the HMRC audit.
4. The draft UK legislation of the 4th Money Laundering Directive was published 17th March and includes requirements that will have significant impacts for Post Office. The extension of the Fit and Proper regime could have a significant impact, however, the exact implications are difficult to assess until clarification is received

POL00401624

from HMRC. If HMRC advise that it includes all agents, and the current fee is applied, this could capture c. 11k individuals with an additional HMRC fee of c. £1.4m per annum. A second significant impact is the requirement to retain physical or electronic copies of customer due diligence documentation for 5 years. As the final legislation has not yet been published, and comes into effect on the 26th June 2017, a transition period is expected.

Input Sought

The RCC is asked to review this report, endorse the recommendations, consider whether further actions should be considered, and approve the report for submission to the ARC.

The Report

HMRC Audit status

5. HMRC met with us on 22nd March to share their audit findings, and advised Post Office that they have identified a number of breaches of regulatory principles, which include:

   - Regulation 7: Application of customer due diligence measures
   - Regulation 8: Ongoing monitoring
   - Regulation 19: Record-keeping
   - Regulation 20: Policies and Procedures
   - Regulation 21: Training

   HMRC are considering whether to levy a penalty in respect of these failings, however as yet we don't have any indication as to timing or amount. The HMRC Anti Money Laundering Supervision team will consider the extent of Post Office failures when establishing potential breaches of the Regulations and whether penalties are appropriate. HMRC have requested that Post Office supply data in relation to bureau de change transactions >€1,000 from January 2015 to August 2016 to determine the extent of breaches.

6. At the meeting on 22nd March, HMRC formally advised Post Office that the penalty for the historic branch registrations filings will be c. £785k, and that a pre-penalty notice would be issued, although this has yet to be received. HMRC also advised that Post Office will not be transferred to the self-service premises registration portal this year. No changes to registration process are therefore required at this stage.

7. HMRC also provided a letter to confirm that they have completed their internal review as to whether the cash processing previously undertaken by Supply Chain for MSB clients was within scope of regulation as a 'Money Transmission' business, and that they have concluded that the published HMRC Guidelines around 'money transmission' are ambiguous, and that this activity is therefore out of scope for premises registration and audit.

8. The majority of the issues highlighted by the HMRC audit relate to in branch Bureau de Change services, and in particular:

   - Levels at which ID is taken and captured
   - Inability to capture linked transactions

POL00401624

- Acceptance of €500 notes
- Inability to prevent business transactions and absence of special due diligence procedures to address this; Poor practices re customer due diligence. E.g. collecting hotel addresses for overseas customers
- System limitations which do not prevent transactions above thresholds
- "Sales driven culture evidenced at some large agents could override need to adhere to regulatory requirements."
- Transaction monitoring limited by poor systems therefore expected checks cannot be robustly applied
- Post Office rely on FRES for certain data, but these data feeds are limited

9. Other concerns relate to:
    - Frequent changes in Post Office MLRO – there have been 6 registered in the last 6 years
    - No training of non-branch staff prior to 2016
    - The sanctions that can be applied to branches that are in breach are limited
    - SARs reporting is low given size of network and number of transactions
10. A project team and steering committee have been established by the Bureau de Change product management team to work on an action plan to address the weaknesses identified in the risk assessment. A high level overview of this activity was shared with HMRC when they presented their findings, and there were no gaps identified in planned activity.
11. A further meeting was held with HMRC on the 5th April to review in more detail the actions that Post Office is already taking and progress a suitable action plan to address gaps. At this meeting, HMRC stated that they will work closely with us and further meetings are planned to agree actions, timescales and milestones, with the next on the 16th May 2017. There were some areas of specific output from the meeting:
    - Post Office to update timescales for the current action plan, and initial estimated implementation/delivery timescales to be scoped for Bureau de Change activity
    - An initial milestone has been agreed to ensure that updated training is delivered to all staff by the end of June (back office training was delivered in April, and customer facing training is being delivered 5th-29th May 2017).
    - HMRC have identified missing data in 26k records supplied to them for analysis, and have asked Post Office to investigate. This investigation is ongoing and poor access to data sources is currently delaying resolution.
    - HMRC recommended dropping the Bureau de Change ID limits as soon as the thresholds had been approved internally, even if the capacity/ability to monitor all the data captured cannot be delivered until later
    - HMRC asked that Post Office undertakes a location-based risk assessment in relation to PEPs risks (e.g. branches within Houses of Parliament and near Embassies)
    - HMRC have advised that they will review Post Office Bill Payments activity later in 2017.

POL00401624

12. An AML Steering Group, chaired by the General Counsel has been established to ensure the HMRC action plan is on track and ensure any changes necessary in relation to the 4th MLD regulations (see Regulatory Update below) are implemented.

Financial Crime Risk Assessment Update

13. As per the agreement at the January R&CC, work commenced in February on risk-assessment work on further products and services and is currently on track, although there has been a need to accelerate the risk assessment of POMS and the insurance products under its umbrella, and so this has been incorporated into this work and given priority during April, the action plans in Appendix A give full updates, but in summary:

    - Drop and Go – re-assessment of the residual risk has been completed, with the control strength improving from 18% to 81%
    - MoneyGram – work is progressing
    - GiftCards – progressing to plan
    - Travel Money Card and Postal Orders – work is progressing
    - POMS – Risk Assessment has progressed well and should be completed by mid-May. Following this work, a POMS annual risk assessment and MLRO report will be provided to the July R&CC
    - International Payments – work is due to commence shortly

14. Legal, Risk and Governance have funded Thistle Initiatives to continue with this work until the end of May 2017. A review of capacity to complete the current work programme is being undertaken. Additional resource will be needed to progress any further products and given the fact that HMRC are to review Bill Payments later in 2017, these services need to be reviewed as a priority.

15. There continues to be non-conformance issues in the Network (see Appendix B for details). There were 68 branches where investigations and actions have been taken P7-P12, with 16 which were more complex of which:

    - 8 have had Bureau de Change ID limits reduced. The Fit & Proper status of the postmistress for one of these branches is being reviewed in relation to her taking on a further branch due to ongoing breaches
    - 3 Directly Managed branch non-conformance has been addressed by the RSM and ASM
    - 8 branches have had remedy letters issued by Contracts Managers

16. There are currently 16 branches being manually monitored.

Anti-Bribery and Corruption (ABC) Risk Assessment update

17. As reported in March, the remediation work is being incorporated over the course of 2017. Activity to date has included:

    - Initial review of ABC policy – further work to be undertaken to update and amend to ensure all risk assessment recommendations captured. Draft to be complete June 2017
    - Enhanced year end 2016/17 executive declaration to include ABC controls.

POL00401624

- Enhance gifts and hospitality reporting, recording and monitoring – work has commenced on scoping the requirements for an electronic reporting mechanism that will aid recoding and monitoring.

AML/CTF training update

18. AML/CTF training for all back office employees was launched in April for completion by 21st April. Early indications are that only 53% of colleagues have completed training. A One communication is being drafted to drive completion.

19. The Communications Team requested that the One communication for all colleagues excluded any reference to bonus eligibility, however agreed to issue a short communication for the attention of all line managers, asking them to ensure that their teams pass the test. On receipt of the non-completion MI, they will send a direct email to all line managers with details of those in their team who have not completed. This communication is to advise line managers to speak to impacted staff and advise them to complete training as a matter of urgency and that any bonus payment is contingent on passing this test.

20. Network customer facing training is being launched on 5th May 2017 for completion by 29th May. A short AML/CTF awareness film has been developed, which will be launched around this time to support understanding of AML/CTF in a Post Office environment.

Regulatory updates

21. The draft UK Legislation for the 4th MLD was published for review on the 17th March 2017, requesting feedback by 12th April 2017. The main impacts for Post Office are:

    - Vetting: there are increased requirements for 'fit and proper' testing (including skills, knowledge and expertise of the individual to carry out their function effectively, as well as conduct and integrity requirements) which are likely to have to be rolled out across the directly managed branch and postmaster population and require annual review. It is unclear the extent to which these will apply to assistants and multiples, and Post Office have requested clarification as to the application of the requirements. This has also been raised with HMRC, but as yet they have no clarity internally as to how this test will be administered or applied. Clearly this requirement would present both an operational and financial burden to Post Office. The Financial Crime team have made the current Vetting Project team aware
    - Copy documentation for customer due diligence needs to be kept during the relationship and for 5 years after a relationship has terminated. For Bureau de Change transactions that require customer due diligence (currently £5k and over, but will reduce to £2k and over following HMRC audit recommendations), Post Office will need to identify a suitable eKYC solution, as retention of paper copies in branch is not an option
    - Any penalty levied will be published without delay and remain for 5 years. For Post Office, it is not yet clear what this will mean in relation to the premises registration penalty, or any penalty levied by HMRC in relation to the regulatory breaches they have identified. The issue has been raised with HMRC
    - HM Treasury and Home Office will issue a new national risk assessment by June 2018, with each supervisor assessing and reporting on the AML/CTF risks in the sectors and businesses they supervise. This will likely impact

POL00401624

organisations interpretation of the requirements of the regulations – i.e. there may be further amends we need to make on our approach dependant on the outcome

- Regulated organisations must undertake a full risk assessment that covers customers, transactions, delivery channels, products and services, and geographic areas and keep this up to date and available for their supervisory authority. Post Office will need to ensure this is fully documented and kept up to date. The risk assessments undertaken to date will meet this requirement, however these will need to be undertaken for all products and services and continually maintained
- Policies, controls and procedures must include risk management practices, internal controls, CDD and the monitoring and management of compliance with these. Post Office will need to have better documented controls across the business, and the risk assessment work will partially address this
- Policies, controls and procedures must specify additional measures to prevent ML and TF use of products and transactions that might favour anonymity. This may impact Post Office for example, top-up services, the majority of Bureau de Change and Giftcards are anonymous
- Occasional transaction limit stays at €15k, and the JMLSG guidance still says three month period is appropriate
- The maximum amount that can be stored on a non-reloadable electronic device is €500 as long as it can only be used in the UK, however, the limit reduces to €250 if it can be used abroad. Businesses must also ensure that no more than €100 can be redeemed in cash. This will impact Giftcards and Post Office will need to establish what GVS are going to do and how this may impact branches.

22. There has been no further guidance or update relating to the Fifth Money Laundering Directive announced on 30 November 2016 and the updates given in March remain current.

23. The Criminal Finances Bill is still progressing through parliament and the updates given in the January MLRO report remain current.

POL00401624

Appendix A – Action Plans

Status key:

- Green – on track and no issues expected
- Amber – some delays but no significant or material issues
- Red – significant delay or material issues or potential regulatory sanction

Risk Assessments:

Activity	Due Date	Status	Comments
Bureau de Change	End January	Complete	Report and recommendations issued to product management – see remediation plan
Drop & Go	Mid May	Green	The report, product information pack and assessment is being sent to the product team for sign-off and progression of risk exception reporting. Control strength has improved from 18% to 81%
MoneyGram	End May	Amber	Some delays in obtaining required information from MoneyGram. With product management to obtain further information for product information pack so that residual risk can be re-assessed.
GiftCards	End May	Amber	Some delays in establishing regulatory status with GVS contract and reviewing documents. Information from GVS now received and with Legal for review
Postal Orders	End May	Amber	Work has commenced and is progressing, provision of initial assessment and draft documents and initial meeting with Postal Order product manager
Travel Money Card	End May	Amber	Not yet started due to timing of launch of multi-currency card and impacts of early 'teething issues' in live environment. Scheduled to commence shortly
International Payments	End May	Amber	Delayed start due to work on other assessments and availability of product manager time (also looks after MoneyGram)
POMS	End May	Green	POMS risk financial Crime risk assessment due to be completed end April and ABC risk assessment by mid-May. On track
Bill Payments (19 separate services)	TBA		Given HMRC intention to review later 2017, this needs full risk assessment and the funding to enable this
Financial Services Products	TBA		29 products across Banking, Savings, Cards, Mortgages, Insurance and top up services - to be prioritised/funded

Remediation Activity:

Activity	Due Date	Status	Comments
Bureau de Change	TBA	Amber	Project team established, but BA leaves business beginning of May so there will be transition to new BA who starts end April. Steering committee established. Requirements being scoped and a Change Request for some 'quick fixes' for Horizon submitted. Decision to remove €500 note service.
Drop & Go	July	Not started	Product team to sign-off residual risk, risk exception to be drafted and approved for a small number of control weaknesses that still exist.
MoneyGram	TBA	Not started	Dependant on assessment of residual risk
GiftCards	TBA	Not started	Dependant on assessment of residual risk
Postal Orders	TBA	Not started	Dependant on assessment of residual risk
Travel Money Card	TBA	Not started	Dependant on assessment of residual risk
International Payments	TBA	Not started	Dependant on assessment of residual risk
POMS	TBA	Not started	Dependant on assessment of residual risk

POL00401624

Other AML activity:

Activity	Due Date	Status	Comments
AML/CTF Policy Review	July 2017	Amber	Although annual review due by end March, awaiting publication of new legislation to ensure all relevant information is captured
ABC Policy Review	March 2017	Amber	Review commenced but resource issues Feb/March
Financial Crime Policy Review	March 2017	Amber	Review commenced but resource issues Feb/March
Policy Gap Analysis	July 2017	Not Started	Dependant on completion of policy amends
Policy control gap action plan	August 2017	Not Started	Dependant on completion of policy amends
PEPs and Sanction Policy	July 2017	Not Started	Draft in line with new legislation and risk assessment outcomes
Review of 4th MLD	June 2017	Amber	Draft legislation reviewed and comments fed back. Awaiting publication of final legislation
4th MLD Action Plan	TBA	Not Started	Dependant on timing of publication of legislation
HMRC Annual Premises Registration	June 2017	Not Started	Awaiting HMRC advice to commence process
HMRC Audit Action Plan	TBA	Green	Initial meetings with AMLS and further meeting May 16th to progress
Risk Appetite Review	TBA	Not Started	Dependant on outcomes from residual risk assessments to provide evidence to support appetite changes
Enhanced AML/CTF training	May 2017	Green	Back Office delivered, Customer Facing Network being delivered 5th May.
POMS and Post Office MLRO reports	July 2017	Not Started	
Enhance Gifts and Hospitality reporting and recording	TBA		
Enhance product and service online risk assessment tool	TBA		

POL00401624

Appendix B – Branch Non-conformance P12 2016/17

Month Identified	Branch	Issue	Action
March	GRO	- First Rate Exchanges Services raised concerns regarding the low bureau transaction volume but high average transaction value. - - High volume of transactions identified just below the £5,000 ID threshold	- Investigation and telephone interview completed by the Financial Crime team. - Remedy Letter sent to PM by the Contracts Manager.
March	GRO	- First Rate Exchanges Services raised concerns regarding the low bureau transaction volume but high average transaction value. - High volume of transactions identified just below the £5,000 ID threshold	- Reduced ID threshold of £2k imposed - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.
March	GRO	- First Rate Exchanges Services raised concerns regarding the drastic increase in Bureau sales in the last 6 months. - High volume of transactions identified just below the £5,000 ID threshold	- Reduced ID threshold of £2.5k imposed - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.
March	GRO	- First Rate Exchanges Services raised concerns regarding the high volume of Bureau sales just below the £5,000 ID threshold	- Reduced ID threshold of £2k imposed - Manual monthly monitoring is being completed. - Remedy Letter sent to PM by the Contracts Manager.
March	GRO	- Postmasters took over branch in August 2016 but did not complete AML Compliance training. - Postmasters delegated on-boarding training to the officer in charge. - Network Operations Advisor failed to identify this during the transfer of the branch.	- Network Operations Admin Team advised of failing - Learning and Development team contacted regarding the on-boarding training process. - Remedy Letter sent to PM by the Contracts Manager.

POL00401624

5.4) Financial Services Conduct Risk Update

Author: Jonathan Hill Meeting date: 4 May 2017

Executive Summary

Context

1. This paper updates the Committee on current risks and actions in respect of conduct risk. One of the key risks on the FS Risk register (also reflected in the Post Office and POMS risk registers) relate to conduct risk. Conduct risk in the regulated financial services context refers to risks to customers from poor product design, distribution and selling processes as well as those risks relating to poor product fulfilment.
2. The Network Conduct Risk Action Plan, agreed between BoI and Post Office and incorporating the requirements from POMS, has completed except for the Enhanced User Management project, which is subject to separate project management and oversight and due to be rolled out in October 2017.

Questions this paper addresses

3. This paper provides an update on the key conduct risks and how they are being managed.

Conclusions

4. Although the business faces some conduct risk challenges, some of which are referred to below, they are being managed within the overall risk appetite. Post Office has an averse risk appetite for not complying with law and regulations or deviation from business' conduct standards. Key assurance on this is provided through the MI dashboards and reports from BoI and POMS.
5. However, there remain challenges from changes to the business model, including regulatory changes, which require on-going focus to maintain conformance and compliance.
6. Post Office, through its Principals, operates in an environment where the regulator is increasingly prepared to take action against individuals in pursuit of its regulatory objectives.

Input Sought

7. The R&CC is asked to note these developments.

POL00401624

The Report

Key Risks, governance and management information

8. Conduct risks are measured and reviewed by FS&T Risk together with our Principals on an on-going basis and management information is provided on the key risk areas. These are reviewed at the BoI-Post Office Customer and Conduct Risk Committee and POMS-Post Office Joint Compliance Committee, which meet monthly

Current risks and issues

9. Customer Relationship Managers (CRMs)

10. The Post Office ARC at the March meeting asked FS&T to explain more about the CRM programme, its controls and how it ensured that advice was not given to the customer.

    We now have 377 Customer Relationship Managers live serving customers with tablets and are on track to reach 500 in May

    CRM control environment:

- All live CRMs and the Post Office Area Sales Performance Managers (ASPM) have been trained in compliant introductory conversations
- Once live, CRMs are monitored in line with the T&C Framework supported and coached by an ASPM.
- Ongoing product specific "Product Knowledge Tests" are completed through direct access to the online CRM learning academy
- All CRMs continue to be monitored through Video Mystery Shopping and Customer Validation Calls for both quality of Customer Experience and Compliance.
- Poor outcomes are reported and actioned through the ASPM coaching structure including any comments that could be construed as advice would be considered here.
- FS&T Risk operate 1st review and control for CRM conduct and compliance risks.
- Tablet content is reviewed and approved by FS&T Risk and our Principals before go-live.

Both the BoI and POMS receive compliance information monthly at their respective Customer and Conduct and Joint Customer Conduct Committees.

Cash Savings Remedies

11. From 1st December 2016, all savings providers have been required by the FCA to provide at the point of sale prescribed information in the form of a standardised summary box. This is to ensure customers have the appropriate information they need to be able to compare products.

12. In order to facilitate a more responsive and cost efficient rate change process in Post Office, a decision was taken to supply this regulatory information to customers in a separate Summary Box leaflet, rather than to include it within the product application pack.

POL00401624

13. Since Post Office Money went live with the Summary Box leaflet to circa. 4,600 branches, initial levels of conformance with the new requirements were varied. The teams have worked closely to ensure branch colleagues understand and conform to the compliance requirements, and are currently running at 78% conformance.

14. The relevant savings material is being updated with a sleeve at the front for the summary box to be inserted into. This should enable high levels of compliance to be maintained. These changes will take approximately two months to deliver. The outcome of this activity will be reviewed at the C&CRC in July 2017.

Future issues

FCA Business Plan and Risk Outlook.

15. The FCA has published its annual business plan and key risk outlook. Its cross sector priority areas of focus include firms' culture and governance and consumer vulnerability and access to financial services. FS&T have undertaken significant work on the importance of embedding an appropriate culture and how we interact with customers through the network conduct risk action plan. This work will continue in the current FS&T work plan.

16. In addition we need to re-focus and agree our vulnerable customer policy to articulate our approach and to manage the demands of our stakeholders who have requested our approach to this. The updated draft policy will be presented to the RCC in July 2017.

Senior Managers and Certification Regime

17. The Senior Managers and Certification Regime will expand to all FSMA regulated firms by 2018; the precise timetable remains unclear but an update paper is expected from the FCA in Q2 2017.

18. Firms will need to put in place a 'Statement of Responsibilities' map, recording the allocation of responsibility to a senior manager for every part of its business areas and management functions. It will also need to identify any significant management/material risk takers that will be 'certified persons'. Firms must certify these as 'fit and proper' on an annual basis. There are also conduct rules for all staff undertaking regulated business under this regime.

19. It still remains unclear what the precise requirements will be for Appointed Representatives, but for POMS planning is already taking place to work through the implications. FS&T Risk is working with POMS to ensure that we are supporting the implementation of SM&CR in POMS.

Insurance Distribution Directive

20. The FCA has recently published a consultation paper outlining the requirements to be in place for February 2018. These include new requirements on a customers' best interests rule, record keeping, commission disclosure and the training requirements for the new regime (15 hours CPD).

21. This could have significant impact on how insurance products are sold and intermediated. POMS is driving a project group to assess and implement the changes with FS&T risk and the wider network.

POL00401624

Jonathan Hill
Head of FS&T Risk & Regulation

May 2017

POL00401624

Health and Safety

Authors: Martin Hopcroft Sponsor: Al Cameron Meeting date: 4th May 2017

Executive Summary

Context

1.1 The Risk & Compliance Committee requested a regular update on our management of risks around the health and safety of our people and customers.
1.2 Health and Safety performance is reported monthly to the Group executive and at each Board meeting, together with information on health and wellbeing.
1.3 Accountability for safety is with Operations, recognising that the greatest risks are to our people in the field.
1.4 Our Health & Safety performance has improved significantly in the past 6 years and we have a rolling 3-year plan to drive health and safety compliance and year on year risk reduction, targeting a reduction in four key safety metrics: accidents; lost time accidents; days lost; and personal injury claims.

Questions this paper addresses:

2.1 What is going well across health and safety and what is not going so well?
2.2 What are we doing to mitigate the key risks, including driving and robberies?
2.3 Are there any significant emerging risks?

Conclusion:

1. Performance continues to remain strong for all four of the key **health and safety metrics**, including absence accidents and lost days (see Report-H&S Metrics).
2. Mitigating action has reduced road risk which remains at a low level. Robberies increased last year after an unusually low level in 2015-16. A number of additional activities are underway.
3. Additional Property H&S **training workshops** have been delivered to Persons in Control of Directly Managed branches to enhance understanding of responsibilities and improve compliance. With almost 100% attendance, feedback from Branch Managers has been very positive and encouraging. 121 coaching is being provided to Supply Chain Pipeline Shift Managers (Apr-May).
4. Following the restructure of the GE and direct reports, individual 'deep dive' H&S sessions will continue to all lead teams. We are undertaking a stand back review of safety priorities across the business and will report to GE in May.
5. The optimal balance of reporting and oversight will be re-considered during Q1 17/18, taking into account the Board, ARC, GE and the Safety Committee.

Input Sought

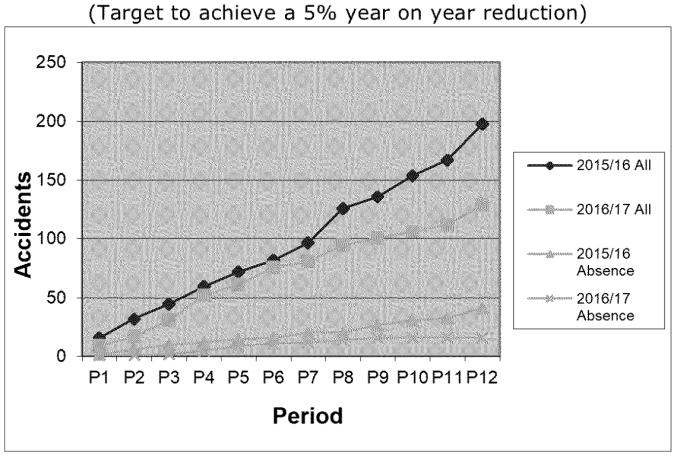
The Risk & Compliance Committee are requested to **note** the update on safety.

POL00401624

The Report – H&S Metrics

Summary of Safety Performance - YTD Period 12 (Mar 16/17)

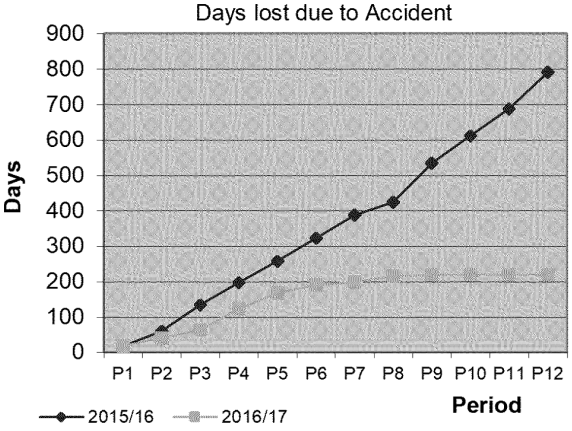
All Accidents – YTD Cumulative at Period 12
(Target to achieve a 5% year on year reduction)



Accidents have reduced by 35% and **Lost time accidents by** 61% YTD P12 (Mar 2017) v 15/16

Lifting / Handling related accidents have reduced about 50% in 2 years.
A lower number of accidents were reported this Winter.
Big improvement in 'lack of attention' related incidents reduced by 50% compared to 2015/16

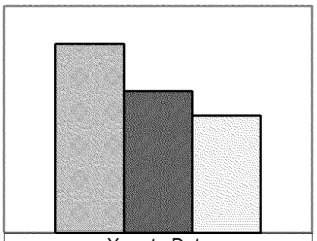
Days lost due to Accident



Post Office lost days have reduced 71% (219 in 16/17 v 792 in 15/16)
DMB lost days P12 YTD : 45 (316 in 2015/16)
Supply Chain lost days P12 YTD : 174 (470 in 2015/16)
Support lost days P12 YTD : 0 (6 in 2015/16)
Trauma days lost: Supply Chain P12 YTD: 144 (302 in 15/16)

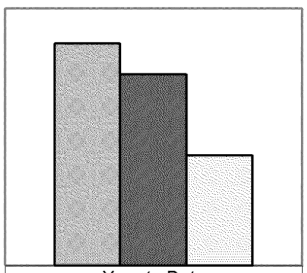
Post Office CViT Robberies – P12 (Mar 17)
There have been 19 incidents reported in 2016/17 compared to 15 in 2015/16 which was an exceptionally strong year, however, this is a reduction on numbers reported in 13/14 and 14/15. There were no incidents reported in December, January and March and 1 incident reported in February. Possible reasons for the reduction are new delivery and collection times and routes and activity across the industry shifting towards ATM related attacks which are on the increase.

Directly Managed Branch
Accidents YTD P12



	Year to Date
14/15	100
15/16	75
16/17	62

Supply Chain Accidents YTD P12



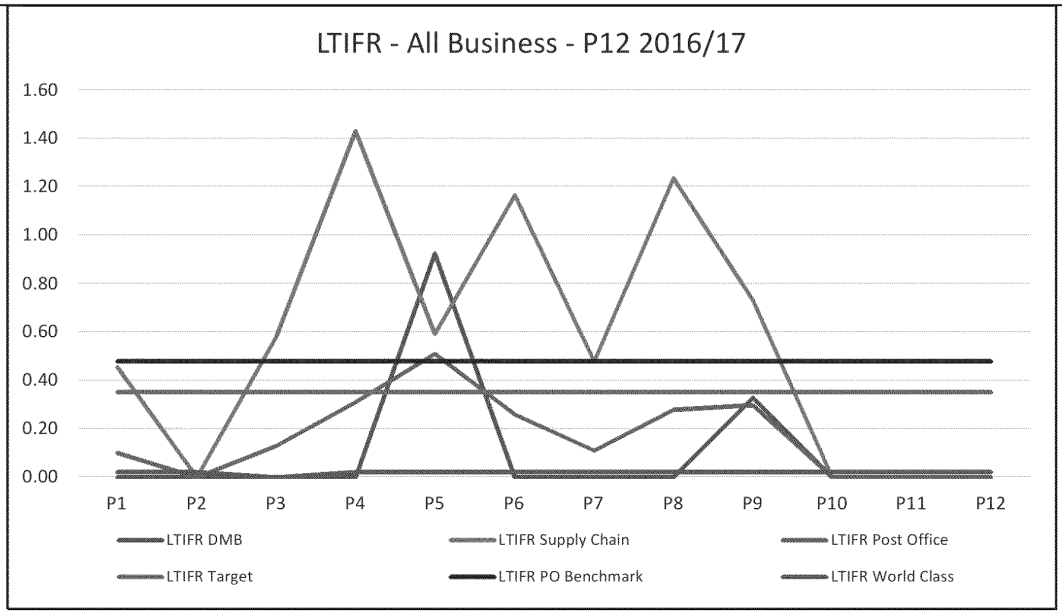
	Year to Date
14/15	121.0
15/16	104.0
16/17	60.0

Post Office (All branch types) Robberies – P12 (Mar 17)
There were:
18 incidents in November v 12 (15/16),
19 incidents in December v 11 (15/16),
20 incidents in January v 9 (15/16)
16 incidents in February v 9 (15/16)
14 incidents in March v 9 (15/16)

(152 incidents in 2016/17 v 104 in 2015/16)

A review of causation and mitigating activity is being undertaken by the Security Team and a paper being prepared for GE with a discussion at the GE Sub Committee in May.

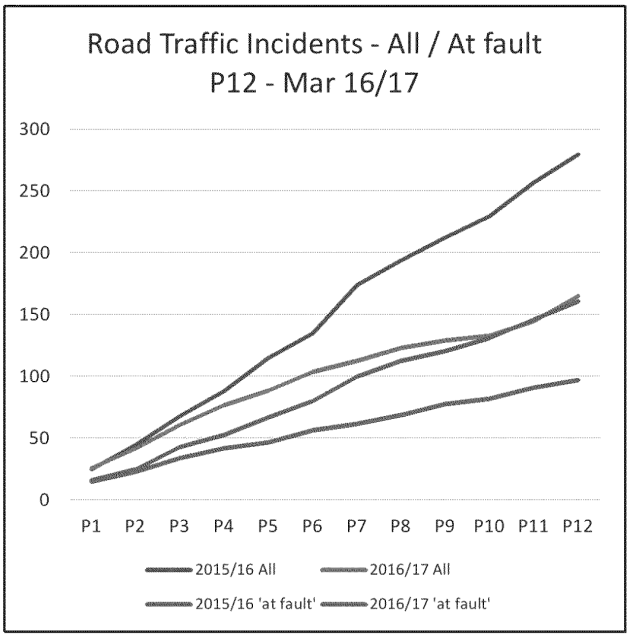
POL00401624



Lost Time Injury Frequency Rate (LTIFR)

Supply Chain
YTD P12 – 0.586
2015/16 out turn – 1.042
2016/17 target – 0.990

All Post Office – Employee
YTD P12 – 0.168
2015/16 out turn – 0.370
2016/17 target – 0.350
PO Benchmark – 0.480



Current road risk performance has improved by 41% compared to P12 YTD 2015/16.

'At fault' incidents are also down by 40% P12 YTD (Mar 17).

New providers have been confirmed for maintenance and accident management for Commercial fleet and for provision, maintenance and accident management of Business Car fleet. Enhanced MI and accident analysis expected from 2017/18 as well as improved training and compliance checks.

The Mobile Phone Policy has been communicated with additional measures being considered by the GE H&S Sub Committee in May.

POL00401624

Summary of Wellbeing Performance - YTD Period 12 (Mar 2016/17)

- The overall attendance level reduced slightly to 96.4% YTD at P12 (Mar 2016/17), as short term absentees return to work and long term cases are resolved.
- There has been a recent increase in the level of absence reported in Directly Managed branches and Supply Chain, due to short term (especially respiratory related cases). Seasonal colds and flu have continued at a higher level for 3 months and not dropped off in P10/11 in line with the usual seasonal trend, however there has been an improvement in P12 with attendance returning to a respectable level of 96.7% at year end.
- Mental health related absences remain the most common cause of long term absence (15% incidents and 30% lost days) however, trend remains stable at P12 and overall lost days due to mental health have reduced. Proactive activity across the business, including 'positive mental health awareness' sessions being held at the FSC Chesterfield and Supply Chain and a specific Time to Talk Teamtalk delivered in Directly Managed Branches on 28th March.

Business Area Absence Performance v Target – YTD 2016/17

	Period 01	Period 02	Period 03	Period 04	Period 05	Period 06	Period 07	Period 08	Period 09	Period 10	Period 11	Period 12	Y.T.D Totals	Gross Hours Target
CENTRAL	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**1.9%**	**0.0%**	**0.0%**	**0.0%**	**0.3%**	**0.0%**
COMMERCIAL	**0.4%**	**0.1%**	**0.1%**	**0.0%**	**0.0%**	**0.1%**	**0.3%**	**0.9%**	**0.0%**	**0.0%**	**1.1%**	**0.0%**	**0.2%**	**0.4%**
FINANCE	**3.5%**	**3.2%**	**3.4%**	**3.5%**	**2.9%**	**2.8%**	**3.7%**	**3.6%**	**3.7%**	**3.8%**	**3.8%**	**2.8%**	**3.4%**	**3.5%**
FIN: CIO	0.0%	0.0%	1.5%	1.2%	0.0%	0.0%	0.0%	0.0%	2.6%	2.5%	3.0%	0.0%	0.7%	**3.5%**
FIN: SUPPORT SERVICES (ALL)	4.6%	3.3%	3.2%	3.0%	2.6%	2.9%	4.1%	5.0%	4.8%	3.8%	3.9%	2.8%	3.8%	**3.8%**
FIN: SS FSC	3.9%	2.6%	2.4%	2.8%	2.4%	1.6%	5.1%	7.5%	6.2%	3.8%	5.4%	3.8%	4.0%	**3.4%**
FIN: SS CONTACT CENTRES	8.4%	4.5%	4.2%	3.6%	2.3%	2.9%	4.0%	4.8%	3.6%	3.3%	3.5%	3.2%	4.2%	**6.7%**
FIN: SS HRSC	2.4%	3.4%	3.8%	3.0%	4.1%	5.1%	5.3%	4.4%	6.0%	4.7%	3.0%	2.0%	3.9%	**2.6%**
FIN: SUPPLY CHAIN	3.4%	3.4%	3.6%	3.9%	3.2%	3.0%	3.9%	3.5%	3.6%	4.0%	4.3%	3.5%	3.6%	**3.7%**
SALES & NETWORK	**3.3%**	**3.0%**	**3.1%**	**3.6%**	**4.0%**	**4.2%**	**4.7%**	**4.4%**	**4.9%**	**4.2%**	**4.2%**	**3.9%**	**4.0%**	**3.2%**
SN: FIN DIR NET & SALES	0.0%	0.4%	0.0%	0.0%	0.0%	1.0%	2.9%	2.1%	0.0%	0.0%	0.0%	0.0%	0.6%	
SN: NETWORK AGENCY SALES,SVCES & TRANSFORM	6.2%	1.8%	4.3%	5.6%	4.1%	5.3%	7.6%	6.8%	7.2%	5.5%	2.2%	3.2%	4.7%	
SN: DMB SALES	3.7%	3.4%	3.3%	4.0%	4.5%	4.6%	5.1%	4.8%	5.1%	4.5%	4.7%	4.3%	4.3%	**3.5%**
SN: SALES DIRECTOR	3.9%	2.5%	3.2%	2.9%	2.5%	3.2%	4.1%	2.8%	4.5%	3.4%	4.0%	4.2%	3.3%	**2.9%**
COMMUNICATIONS & CORPORATE AFFAIRS								**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	**0.0%**	
HUMAN RESOURCES	**1.6%**	**1.7%**	**1.3%**	**1.1%**	**1.4%**	**1.9%**	**0.6%**	**0.6%**	**1.2%**	**1.5%**	**0.0%**	**0.0%**	**1.2%**	**1.1%**
HR: DIR	0.0%	3.4%	3.1%	3.1%	0.2%	0.0%	0.0%	1.2%	2.4%	1.2%	0.0%	0.0%	1.4%	**0.3%**
HR: LEARNING, RESOURCING & TALENT	4.9%	2.6%	0.7%	0.0%	3.1%	2.3%	0.7%	0.0%	0.0%	1.9%	0.0%	0.0%	1.4%	
GENERAL COUNSEL	**0.3%**	**0.4%**	**0.0%**	**2.2%**	**1.3%**	**0.6%**	**1.3%**	**2.2%**	**2.8%**	**1.9%**	**1.9%**	**2.5%**	**1.5%**	**1.8%**
GC: INT AUDIT	0.0%	0.0%	0.0%	1.5%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.2%	
FINANCIAL SERVICES	**0.6%**	**2.1%**	**2.2%**	**2.1%**	**1.6%**	**1.6%**	**0.0%**	**0.6%**	**0.8%**	**0.1%**	**3.1%**	**3.0%**	**1.9%**	**2.8%**
FS: POST OFFICE MONEY	0.0%	0.0%	0.0%	0.3%	0.0%	0.0%	0.0%	1.3%	0.0%	0.0%	0.0%	0.0%	0.1%	
BUSINESS TRANSFORMATION	**0.6%**	**1.6%**	**0.0%**	**0.6%**	**0.2%**	**0.9%**	**3.4%**	**3.4%**	**4.4%**	**3.8%**	**1.4%**	**0.0%**	**1.8%**	**3.0%**
BT: CHANGE MANAGEMENT	0.6%	1.8%	0.0%	0.7%	0.2%	1.0%	3.7%	3.7%	#DIV/0!	4.3%	1.6%	0.0%	1.8%	
Post Office Ltd	**3.2%**	**2.9%**	**3.0%**	**3.4%**	**3.4%**	**3.6%**	**4.1%**	**3.9%**	**4.2%**	**3.8%**	**3.8%**	**3.3%**	**3.6%**	**3.3%**

POL00401624

The Report

2.1 What is going well across health and safety and what are the current activities?
2.2 What are we doing to mitigate the key risks, including driving and robberies?

SAFETY

Performance continues to remain strong across all key health & safety metrics, including absence accidents and lost days (see Report–H&S Metrics). Current activities include:

1. **Person in Control (PiC) Training -** Refresher PiC training has been undertaken by all Supply Chain and DMB Managers. Additional Property H&S training workshops have been delivered to DMB Managers with very positive feedback. Team Talk session is being developed for all colleagues in DMBs to ensure minimum awareness and support for H&S.
2. **Property related risk (As reported in the Property Compliance Report)**
   - The overall level of risk at year end is low with property compliance 96.55%.
   - All planned Asbestos removal has been completed.
   - All High and Medium actions from the fire risks assessments are closed.
   - Our site audits have evidenced that we are managing our buildings and housekeeping is improving.
   - Revised log books have been agreed for distribution to sites early Q1 17/18
3. **Health & Safety Activity Calendars -** To ensure Health & Safety activities are undertaken, H&S calendars have been updated and launched for 2017/18. H&S BPs attending Lead Team meetings to help raise awareness and compliance.
4. **Road Risk -** The Road Risk Forum has reviewed priorities and performance with a presentation planned for the GE Sub Committee deep dive on May 5th.
5. **Security / Robbery Risk -** A report is being developed by Security Manager to support a GE discussion in May, due to the increase in number of Post Office robberies November to March. However, CViT related incidents remained low in Q4 (18 in Q4 14/15, 11 in Q4 15/16 and only 1 incident in Q4, 16/17).
6. **Hosted Directly Managed branches -** H&S team members are attending branch site meetings to provide advice and support to project teams and Branch Managers prior and during transfer. Post Office and WHSmith H&S Managers and Property Compliance Managers are working closely to share processes and documentation.

ENVIRONMENT

1. The Environmental Tactical Group is currently reviewing policy and gathering energy, recycling and carbon data for the Post Office year end review.
2. Guidance has been provided to 'Persons in Control' for the management of waste and raise awareness of the risk of receiving fixed penalties/enforcement notices.
3. A range of short term and long term action is being reviewed by the Environmental Tactical Group (H&S, Property, Legal) for discussion at the H&S deep dive in May.

WELLBEING

1. Health & Safety team are raising awareness of available resources at Support Centre, Supply Chain & Directly Managed team meetings and during Supply Chain visits.
2. Mental health awareness 'Time to Talk' approach is being rolled out to all areas of the business, including use of the TeamTalk session to encourage the conversation at Directly Managed Branches and Supply Chain sites.

POL00401624

3. The Occupational Health provider is developing further guidance regarding 'Mental Health First Aid' training for volunteers across the business (approx 60).
4. Health Checks will continue to be offered to all employees (either Kiosk or Mobile)
5. The range of OH services available has been reviewed and approved
    - Launch of the Post Office Wellbeing Portal in May, enabling access (externally and internally) to all services and resources through one landing page.
    - Extension of the absence 'case management' pilot, OH Assist™ Advice Plus.
    - Training provided to Support Centre call advisers and team leaders for 'difficult' and traumatic calls to be extended to Contract & Security Managers.

What additional activity has been undertaken to address specific risks?

1. **Compliance to Driving and Mobile Phone Policy -** Policy has been communicated on the Intranet, H&S home pages and reinforced at team meetings. Developing an online training module for business drivers. A communication will be issued to drivers claiming business mileage to capture a record that the policy read and understood.
2. **Environmental Policy -** The Property Compliance and H&S teams are working closely with Legal, Servest and IT to minimise risk associated with general waste. Guidance has been issued to Persons in Control through workshops and coaching.
3. **Security and lone working in Support Centres -** H&S, Property and Security Managers are reviewing the personal security arrangements in place at all Support Centres and satellite locations. Will be discussed at the May H&S deep dive session.

2.3 Are there any significant emerging risks for 2017?

1. **Simplify Supply Chain, Support Team OD, DMB Development Programmes**
    - H&S BPs are monitoring absence, accident trends and causation and working closely with lead teams, providing training to ensure the focus on safety, attendance management and wellbeing continues.
    - Induction programme including H&S content is under review to ensure all line managers of new managers and employees complete the H&S Checklist.
    - Support and training is being provided to Supply Chain Shift Managers to prepare for external OHSAS 18001 audit, ensuring records are brought up to date, managers are upskilled and prepared for the external interview.
2. **Property / IT – Disposal of hazardous waste -** There are concerns on how we dispose of IT hazardous waste, in particular printer cartridges and we are at risk of potential prosecution. To rectify, current arrangements will be communicated ie. For back office printers, redundant electrical equipment. All DMB PiCs have been instructed to safely retain items in the short term, esp. Horizon printer ink cartridges, pending instruction, once a process to recycle all items has been agreed.
3. **Road Risk -** A driver in Supply Chain informed us that his licence had been removed for alcohol dependency. There is no evidence that he has ever driven drunk and he denies that this has been the case. The issue of whether we should undertake alcohol and drugs testing has been considered previously and it was concluded that we should not. We have therefore brought forward a review of this decision encompassing new technology which could use fingerprint testing as a permission to release keys rather than a random test. In addition, we have already asked the Network Operations Director to review our safety procedures for people, such as the operations field team, who drove either their own or company cars for Post Office business." This will be discussed further at the H&S deep dive meeting in May.

POL00401624

5.6) Change Risk Update

Author: Jenny Ellwood Sponsor: Angela Van Den Bogerd Meeting date: 4 May 2017

Executive Summary

Context

This report provides an update on the key risks being managed within the Change Portfolio. It also provides a high-level analysis of the Change risk profile, how the portfolio is performing and the key challenges being faced.

Questions addressed in this report

- What are the top risks currently being managed within the Portfolio and what is the performance of risk management based on the mitigation plans?
- What are the types of portfolio risks and how has this mix changed?
- What is the current churn rate of portfolio risks and what are future projections?
- What is the current risk weighting of the portfolio/how is this expected to change?

Conclusion

1. There has been some slight changes to the top risks reported in March, the Resourcing – Off Payroll has reduced in impact and probability following the completion of a number of mitigations. However the two previously reported risks i) Complex Change Portfolio Delivery and ii) IT Vendor Renegotiation / IT Supplier Capacity remain red and continue to be closely reviewed and monitored.
2. The type and mix of the portfolio, broadly, remains unchanged at this reporting cycle. Portfolio and key Programme risks continue to be regularly reviewed at a monthly risk workshop. A new emerging risk is being explored around how we monitor the external environment we are dropping the changes into. The Communications team have highlighted some changes recently made, which would usually land without any negativity with Agents not being received quite as anticipated this time around.
3. The Portfolio Risks have reduced to 27 and remain consistent with the nature and complexity of the individual projects and the timeline.
4. Confidence remains that the current top risks reported are being managed appropriately and do not currently create substantive risk to our plans. The health checks with each Programme is also allowing us to explore in greater detail, with the Programme leads, the key risks being managed.
5. The current residual risk exposure is tracking within appetite and threshold.

Input Sought

The ARC are asked to note the progress made since the last ARC, the top risks being faced, how they are being managed and mitigated and to advise on any additional areas/topics that should also be taken forward.

POL00401624

The Report

What are the top risks currently being managed within the Portfolio?

1. There are currently 27 open risks being managed at a Portfolio level (a reduction of 4 from the last ARC report in March 2017). The current top risks are:
   i) Complex Change Portfolio
   ii) IT Vendor Renegotiations/Capacity of key IT Suppliers

2. The Resourcing–Off Payroll working Legislation risk has reduced in impact and probability following the completion of the key mitigating actions. A full update is provided later in this report.

3. Work continues to maintain, and in time, reduce the impact and probability of the Complex Change Portfolio Delivery risk. Following the rescheduling of three specific Programmes (Enhanced User Management, Success Factors and Transaction Simplification) delivery activity is now slightly congested in May through to August. However, from a network and agent's perspective, there is nothing to suggest that we cannot deliver in line with the plan and at this stage there are no changes being proposed. However, test capacity is finite and the dependency is that each Programme commences and concludes their testing without any major problems and delays. This area of the plan requires close monitoring.

4. The work on the Integrated Plan continues with the next phase of actions being around the interlocking of the IT Delivery Road Map. This will provide a view of the plan from an IT lens, particularly from an IT capability perspective, both from an internal and an external view from our key third parties. This will enable us to identify any conflicts and then work will commence on how best to mitigate e.g. investing in improving our test rig capabilities. Work continues between the IT Portfolio Manager and the People & Change Director on a review and improvement to the end to end change process. The Technology Architecture team are assisting in reviewing a portfolio management tooling system (ServiceNow) to integrate with the end to end change planning tool.

5. Planning continues on monthly basis when change delivery leads meet to review activities and highlight issues which require resolution

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(iii) Complex change portfolio delivery	The next phase of Transformation will have increased dependencies and interconnectivities leading to more complexity to manage, which if not managed well could significantly impact our execution plans.	**16** **I/L** **4:4**	• Develop single Business/IT Master Plan to schedule/smooth Change Delivery **(May 17)** • Create a single view of all Change **(Complete)** • Ensure clear lines and demarcation of accountability between Change Programmes and Enterprise Portfolio Management activities **(Complete)** • Prioritisation exercise to be completed to identify they key activities to be progressed **(Complete)** • Produce new integrated plan and identify scheduling and hotspot constraints in line with prioritisation exercise above **(May 17)**	May 2017	**12** **I/L** **3:4**

POL00401624

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
			• Implement central dependency tracking to allow increased visibility, management and control **(Complete)** • Analyse high-level dependencies to ensure robustness and integrity of high level plan (**May 17**)		

6. There are two current IT Third Party risks which are closely linked; IT Vendor and Capacity of Key IT Suppliers.

7. With regard to IT vendor renegotiations, since the last ARC the contract negotiations have continued and good progress has been made to align to Fujitsu's new global operating model. A ways of working approach to redesigning the IT operating model has been agreed with Atos. Work will convene in May to transition.

8. There are still significant capacity issues (particularly around testing and people) between suppliers and the Post Office. Work is underway on confirming our demand requirements. This will allow us to provide our suppliers with an increasingly accurate medium to long term forecast of demand against which the suppliers will be able to build additional capacity and thereby remediate these capacity issues. In the interim we are managing these issues by scheduling within existing capacity constraints. We acknowledge this is a sub-optimal solution.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(i) IT Vendor Renegotiations	There is a risk that IT Vendors engagement proves difficult and they display poor behaviours through renegotiations which could impact successful change delivery	**16** **I/L** **4:4**	• Establish Legal support to assist in vendor contract renegotiations **(Complete)** • Hire negotiation and procurement expertise **(Complete)** • Contract Managers are in place to manage transition and ensure Vendor SLAs and commitment is maintained **(Ongoing)** • Leverage GE/Board and other connections **(Ongoing)**	Ongoing	**9** **I/L** **3:3**

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(iii) Capacity of Key IT Suppliers	There is a risk that key IT suppliers cannot meet our change demands due to pace of change and activity concurrency resulting in delays to delivery plans	**12** **I/L** **4:3**	• Secure persistent delivery teams aligned to strategic goals and purpose of POL **(Ongoing)** • Continue monthly reviews with Vendors **(Range of meetings are in place - ongoing)** • Contract Managers to monitor vendor capacity and delivery and escalate issues to TDG and GE **(Ongoing)**	Ongoing	**8** **I/L** **4:2**

9. The Off Payroll working legislation is now in force (6 April 2017). Whilst this risk could have delayed some of our change activities the mitigations which were agreed and managed have helped reduce this risk to an amber position and ensure there were no Post Office change programmes at risk as a result of the new legislation.

10. We now have agreed ways of working with our remaining contractors. Some of the roles are now considered out of scope of IR35 and therefore there has been

POL00401624

no change to their daily rate. Other roles have remained in scope and we reviewed the outcome on a one to one basis. Some have remained on the same daily rate, others we have had to slightly increase to retain the skillset.

11. Work continues with AMS to see if it would be of benefit to the Post Office to buy out some of the contractors and move these to the new resource supplier, Sopra Steria. This will enable us to review the role and if applicable place outside of IR35.

12. Although this is clearly an improving situation, at this stage, we still need to continue to monitor as we cannot be sure that some contractors are not still looking for alternative employment. Second, the full impact on a contractor's income, particularly in respect of employers NI and expenses has still need been seen, at which time we may receive more queries.

Risk Title	Risk	Current RAG	Mitigation Plan	Due date	Target RAG
(i) Resourcing – Off Payroll working Legislation	There is a risk that HMRC legislative changes effective from April 17 cause significant impact to Transformation current resource model.	9 I/L 3:3	• Obtain appropriate legal / tax expert advice **(Complete)** • Work with Business Leads to run through contractor resource and their criticality to the Programmes and develop action plan / contingency approach **(complete)** • Establish level of assurance POL need to complete where POL obtain resource through a third party supplier **(process understood now need to develop operational procedures to support)** • Reforecast change demand to identify required resource and skill requirements for a three month rolling profile **(in progress)** • Continue to communicate to Contractors and GE/Exec **in progress)** • HR to confirm the preferred mix of change resource in terms of perm to contractor **(May 17)** • Review the Contractor Buy out option with AMS **(May 17)**	May 17	4 I/L 2:2

13. A full list of the 27 portfolio risks is shown as an Appendix.

What are the types of portfolio risks and how has this mix changed?

14. At the last ARC meeting there were 31 portfolio level risks. Since then Change has seen a net decrease in the number of open portfolio risks which now stand at 27. This was the result of the closure of 4 risks namely:

- Business process management: this risk related to the efficiency of our Business Processes following the delivery of the Transformation Programme. The risk was closed on the basis that the completed mitigations had brought the current severity and likelihood rating within target and tolerance. Such mitigations included the development of a BAU business process management framework, standards and BPM Centre of Excellence within Support Services. In addition, arrangements had been made to ensure that business process changes will be assessed and agreed by the Design Authority
- Supply Chain: this risk related to the possibility that changes made from the Supply Chain Programme could impact on operational performance in the

POL00401624

wider business areas. This risk had been closed as the programme has almost completed delivery and the risk had not materialised

- Cost of voluntary redundancy: this risk has been reviewed by Finance and has been closed as it as specific to the Supply Chain programme
- Cost Reduction Initiatives impact Transformation requirements: this risk has been closed on the basis that the Strategy to Plan work has been completed, a priority list of activities has been approved and is incorporated within the integrated high-level change plan.

15. A new risk has been added to the portfolio, around data management, which replaced two older data related risks. This risk is around whether the current level of data governance / single source of data within the Post Office is sufficient to support the delivery of change. To explain further some of our change activities will be changing data sources/requiring access to accurate data to develop their requirements. Mitigations have been agreed with the Business Information team which include: i) Programmes engaging as early as possible with Data SME to ensure any data related milestones are accurate and achievable, and; ii) to escalate any problems to the change team for visibility and escalation of this risk if it does impact scope and deliverables.

16. The table below, illustrates how the mix of risks at portfolio level continues to flex and shows the open portfolio risks by severity.

RAG Impact/Likelihood	Minor (1)	Moderate (2-4)	Major (5-11)	Significant (12-19)	Critical (20-25)	Total
Apr-17	0	2	14	11	0	27
Mar-17	0	2	15	13	0	30
Feb-17	0	2	14	15	0	31
Jan-17	0	2	14	16	0	32
Dec-16	0	0	17	18	0	35
% of total (current period)	0%	7%	52%	41%	0%	100%

Figure 1: Please note the minor/moderate risks are managed at a local level and not escalated to the Portfolio view.

What is the current churn rate of portfolio risks and what are future projections?

The next table details the number of risks open and closed over the last 6 months.

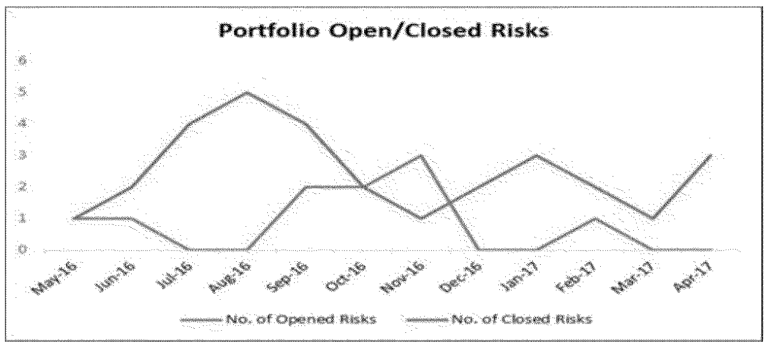


Figure 2: A comparison of open/closed risks (by month)

POL00401624

17. Monthly Programme health checks commenced in April where the key focus was to discuss on a one to one basis with the key Programme and Business leads the main issues, risks, milestones and dependencies together with the cost and benefit realisation activities. These went well and allowed a more detailed discussion, which will be built upon each month to increase visibility and awareness of the challenges, risks and also opportunities in the plans.

What is the current risk weighting of the portfolio and how is this expected to change?

18. Each risk has a weighting score calculated by multiplying their impact/probability scores. When added together this provides a cumulative portfolio score.

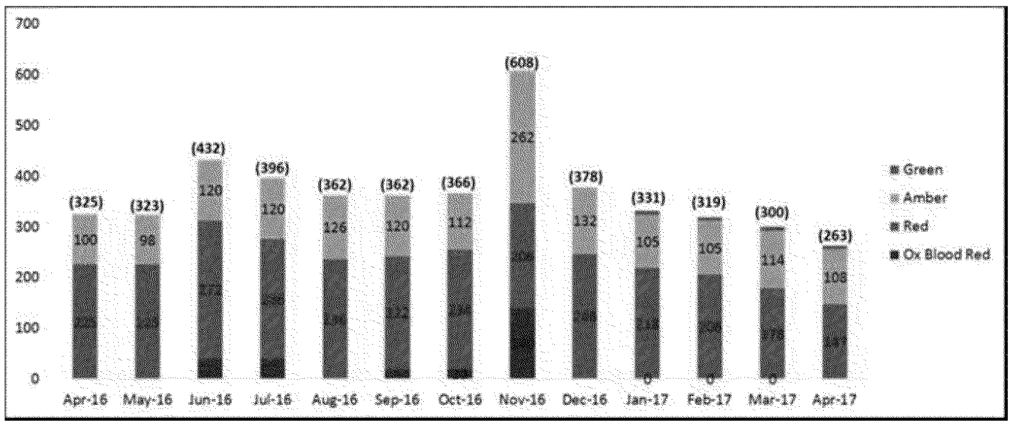


Figure 3: Current cumulative portfolio risk weighting score by month

19. The overall risk severity score has reduced by 12% since March 2017. This has been the result of risk closures. The risks continue to be monitored in line with the change portfolio risk review process.

20. Figures 4 and 5 illustrate the anticipated impact of a reduction in the number of active risks (within the current portfolio) over the next 6 months will have on the residual risk weighting. In part this is because a significant number of the current portfolio risks will reach their target risk weight (which will be in line with risk appetite). This does not taken into account, of course, the impact that newly identified risks will have on the portfolio.

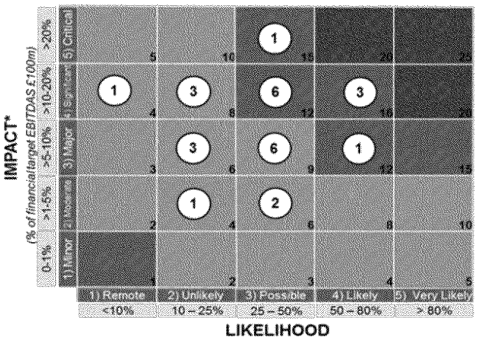


Figure 4: Current portfolio risk weighting (April 2017)

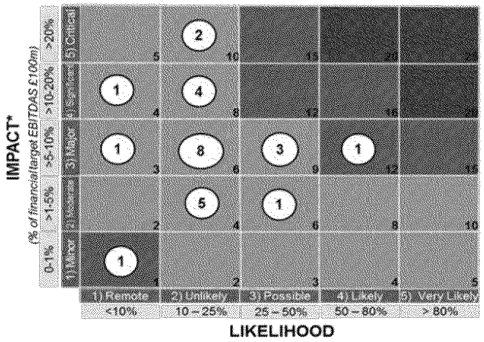


Figure 5: Projected portfolio risk weighting (Nov 2017)

POL00401624

Appendix: Transformation Portfolio risks

	Risk Title	Mar ARC	May ARC	Grid Ranking CURRENT	Grid Ranking TARGET
1	IT Networks Branch and Admin Delivery Risk			16	6
2	IT Vendor Renegotiations	✓	✓	16	9
3	Complex Portfolio Planning & IT Management	✓	✓	16	10
4	IT Networks Branch incumbent supplier proactive engagement			15	10
5	IT Delivery Capability	✓		12	6
6	IT Supply Chain	✓		12	8
7	STRN ePOS Solution Uncertainty			12	6
8	Financial risk - Insufficient Funds to deliver Transformation			12	9
9	Delivery - Integrated Plan Delivery Performance			12	6
10	Capacity of IT Key Suppliers	✓	✓	12	8
11	Data Risk			12	8
12	Resourcing Risk - Payroll Legislation	✓	✓	9	4
13	Transformation Delivery oversubscribed			9	9
14	Portfolio Plan			9	6
15	Unintended consequences on Operational Performance – Process			9	6
16	Availability of Key Skills and Knowledge			9	6
17	Unintended consequences on Operational Performance – People			9	6
18	IT Strategy - Alignment with Transformation			8	2
19	Financial risk - Benefits/Revenue Realisation			8	6

POL00401624

	Risk Title	Mar ARC	May ARC	Grid Ranking CURRENT	Grid Ranking TARGET
20	Deployment of Non-Compliant Solutions/Systems - (Breach of LRC reqts)			8	4
21	Responsible use of public funds			6	1
22	Strategy & Design: Conflict between current BaU and Transformation activities			6	6
23	Accounting & Reconciliation			6	4
24	Reputational Damage - Media risk			6	4
25	Reputational Damage - Political stakeholder risk (local government)			6	4
26	Reputational Damage - Political stakeholder risk (national government)			4	4
27	Poor coordination of communications about change activity with stakeholders and employees			4	4

POL00401624

7. Internal Audit Report

Author: Johann Appel Sponsor: Jane MacLeod Meeting date: 4 May 2017

Executive Summary

Context

The purpose of this paper is to update the Committee on the PO Business As Usual Internal Audit (BAU) and Business Transformation Assurance (BTA) activity and key outcomes. This includes details of the work completed since the last Audit, Risk and Compliance Committee (ARC) in March and progress on the 2016/17 Internal Audit Plan.

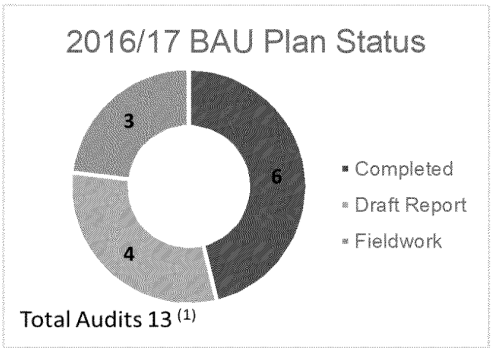
Questions this paper addresses

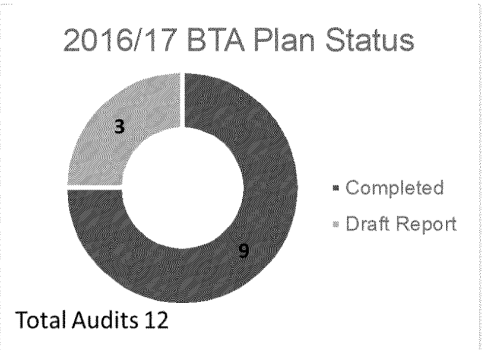
- Is the Internal Audit Plan on track? What progress has been made since the March RCC and ARC meetings?
- What progress is being made with completion of audit actions?
- Have any significant issues arisen that the committee should be aware of?

Conclusion

1. Progress against plan (2016/17):

Two audit reports were issued since the March ARC. A further seven reports are currently being cleared with management for reporting at the May ARC. Current status against the 2016/17 plan is as follows:





(1)Original plan 12 +1 carried forward from 2015/16 + 4 additions - 4 postponed/replaced

Full summaries of 2016/17 Audit Plan Status are included in **Appendix 1a and 1b**.

2. Progress against plan (2017/18):

Although we are still focused on finalising the 2016/17 audit programme, we have also begun to plan and execute the Q1 reviews from the 2017/18 plan. Three reviews are now in fieldwork, while a further four are being scoped.

POL00401624

3. Open and Overdue Audit Actions (as at 26 April 2017):

Audit Action Status:	BAU	BTA
Open (not yet due)	17	9
Overdue (<30 days)	2	5
Total	19	14

4. Significant Issues:

There are no significant issues we believe the committee should be made aware of.

Input Sought

The Committee is asked to note and provide comment as necessary.

POL00401624

The Report

5. Changes to Plan since March RCC and ARC

2016/17 Plan: There was one change to the 2016/17 BTA plan. Following discussions with management, the review of Data Management & Quality was cancelled as this is currently being addressed as part of the Back-office Transformation programme and the GDPR project. It was agreed that Deloitte would provide limited scope advisory work to inform Post Office on best practice for data management and quality. Full plan details can be found in Appendices 1a & 1b.

2017/18 Plan: Following a request from management, a review of the VAT Process was added to the plan.

6. Internal Audit Reviews Completed

We have finalised one BAU and one BTA review since the March RCC & ARC meetings. Following is a summary of the key findings from these reviews:

Audit	Key Messages

Identity and Access Management (Joiners / Leavers / Movers)
Adverse
	• Lack of overall IAM governance (e.g. no ownership of the end to end process, no process diagram).
	• IAM– JML access management responsibilities (RACI) and controls are not clearly and transparently defined.
	• Line managers not well informed about their responsibilities regarding IAM-JML process.
	• Insufficient controls over Joiners, Movers, Leavers, specifically:
	  ○ No assurance that access rights are limited to a need to know basis.
	  ○ HR does not have a full overview of all parties working for PO (employees, contractors).
	  ○ No assurance that access rights are reviewed when someone moves role/function & no periodical access reviews performed.
	  ○ No assurance that leavers' access rights are removed.
	• Data and system owners have not been identified.
	• Non-compliance with the access control standard/policy.

BTA – Business Case Development
Satisfactory (with exceptions)
	• Overall, the application of the OBW methodology has led to an improvement in the quality of business cases submitted and no significant instances of non-compliance with the framework were identified.
	• Some further improvements have been identified related to the framework and associated guidance. Specifically:
	  ○ Programme funding approvals were not consistently tracked;
	  ○ Changes to project costs and benefits were not consistently captured within business cases and associated documentation.

POL00401624

Management have accepted the audit findings and corrective actions have been agreed. Executive summaries of the above two audits are attached as **Appendix 2a & 2b.**

7. Reviews In Progress

Review	Status / Remarks
Financial Reporting Controls Framework (Independent Testing)	Mostly complete - 74 controls tested over 10 processes. Testing of Stock and 3 year-end controls still to be finalised.
IT Controls Framework (Advisory - carried forward from 16/17 plan)	Ongoing – providing challenge and input to the project.
IT Security Transformation (Advisory– carried forward from 16/17 plan)	Ongoing – providing challenge and input to the project.
VAT Process (Addition to 17/18 plan)	Fieldwork – This audit is focussed on the correct application of VAT rules, as well as governance and oversight over the process.

8. Reviews In Planning (Q1 2017/18)

Review	Status / Remarks
Mails Process	Management requested that we bring this audit forward to Q1, with particular focus on the controls over mails segregation and service credits received from RMG.
SAP Success Factors – Payroll (Change)	Being scoped.
SAP Success Factors - Employee Central and EUM (Change)	Being scoped.
PCI Compliance (Change)	Being scoped.

9. Updates on Internal Audit Overdue Actions

As from 1 February we have rolled out an improved audit action tracking process to provide early reminders to action owners of actions that are due within the next month. Action owners are asked to provide a status update and flag where there is a risk that completion dates will not be met. This information is then pro-actively shared with the relevant GE owner.

Audit actions are generally being completed on time. The status of open audit actions at 26 April 2017 was as follows:

BAU Audit Actions:
There were 19 actions open, two of which were overdue less than 30 days. Both actions relate to the Branch Network Sales Training & Competence Review (GE Owner – Nick Kennett). Following Project Finch and the associated restructure of the FS teams and management, a full review of the Frameworks and the related MI have

POL00401624

been postponed until the changes have been implemented. Expected revised completion date is July 2017.

BTA Audit Actions:
There were 14 actions open, 5 of which were overdue less than 30 days. Of the overdue actions, one relates to the Separation PIR (GE sponsor - Rob Houghton) and four relate to the Information Security review (GE sponsor - Rob Houghton / Jane MacLeod). Due to workload and competing priorities, management have requested extension to the deadlines and we continue to track the progress of these actions.

END OF REPORT

POL00401624

Appendix 1b

BTA- 2016/17 Plan Status as at 26 April 2017							Actions			Reporting		Comments
No.	Audit Title	Key Audit Contact	Timing	Revised Timing	Status	Report Rating	High	Medium	Low	Due RCC	Due ARC	
1	End to end Financial management of Transformation	D.Hussey	Q4	Q1	Final	Average	1	8	5	05 May 2016	19 May 2016	Final report issued and presented to ARC.
2	Portfolio Management OE#1	D.Hussey	Q4	Q1	Final	Satisfactory	0	1	2	05 May 2016	19 May 2016	Final report issued and presented to ARC.
3	Digital Programme Mobilisation	M.George	Q1		Final	Adverse	6	1	0	14 July 2016	28 September 2016	Final report issued and presented to ARC.
4	Planning Boot Camps #2	D.Hussey	Q1		Highlight Report	Satisfactory	1	9	15	14 July 2016	28 September 2016	Final report issued and presented to ARC.
5	Communications and Stakeholder Management	D.Hussey	Q1	Q2	Final	Satisfactory	0	2	1	14 July 2016	28 September 2016	Final report issued and presented to ARC.
6	IT Separation (From RMG)	A. Cameron	Q3	Q3	Final	Not Rated (PIR)	6	5	1	03 November 2016	17 November 2016	Final report issued and presented to ARC.
7	Information Security	J.MacLeod	Q3	Q3	Final	Adverse	8	3	6	03 November 2016	17 November 2016	Final report issued and presented to ARC.
8	Winning with Retailers	M.George	Q1	Q2	Final	Not Rated (PIR)				10 January 2017	30 January 2017	Final report issued and presented to ARC.
9	Business Case Development	A. vd Bogerd / A.Cameron	Q4		Final	Satisfactory	0	2	1	09 March 2017	27 March 2017	To be reported at May ARC.
10	Project Expenditure Approval Process (Addition)	J.MacLeod	Q4		Final Draft Report					09 March 2017	27 March 2017	Management request. Information requests delayed fieldwork and report clearance. To be reported at May ARC.
11	3rd Party Vendor Management	A. Cameron	Q3	Q4	Draft Report					04 May 2017	18 May 2017	Merged with BAU 3rd Party Vendor Management audit. Information o/s from ISG and Verizon delayed fieldwork.
12	Target Operating Model	A. vd Bogerd	Q2	Q4	Draft Report					04 May 2017	18 May 2017	Work was suspended pending TOM Board Paper submission (Nov 16). Work re-commenced March 2017.
	Data Management and Quality	J.MacLeod	Q3	Q4	Cancelled							Cancelled due to internal review done in 2016 and a project now on the way to improve governance over data. Deloitte to provide limited scope advisory work.
	Ox Blood' Red rated risk reviews		Q4		Cancelled							
	Support Services Transformation		Q3		Cancelled							
	POCA		Q3		Cancelled							
	Back Office Tower Transition		Q3		Cancelled							

POL00401624

Appendix 1a

BAU 2016/17 Plan status as at 26 April 2017						Actions			Reporting			Comments
Audit Title	Key Audit Contact	Timing	Revised Timing	Status	Report Rating	High	Medium	Low	Co Sec deadline	Due RCC	Due ARC	
Data Protection (Carried over from 15/16)	J. MacLeod	Q2	Q3	Final	Average	0	8	2	03/01/2017	10 January 2017	30 January 2017	
DC Pensions Issue (Addition)	A. Cameron	Q2		Final	Not rated	4	1	0	27/10/2016	03 November 2016	17 November 2016	
Vetting (Addition)	J. MacLeod	Q3		Final	Average	0	2	1	n/a	10 January 2017	30 January 2017	
FS Training and Competence schemes - PO Network	N. Kennett (K. Gilliland)	Q1		Final	Average	1	9	15	03/01/2017	10 January 2017	30 January 2017	
IT Disaster Recovery and Resilience	A.Cameron (J.MacLeod)	Q2	Q3	Final	Adverse [1]	3	5	0	27/10/2016	03 November 2016	17 November 2016	
Identity and Access Management (Joiners, Movers, Leavers)	A. Cameron (M. Kirke)	Q2	Q4	Final	Adverse	6	4	0	02/03/2017	09 March 2017	27 March 2017	
Branch Audit 1st Line (revisit and update)	M.Ellis	Q3	Q4	Final Draft Report	n/a				02/03/2017	09 March 2017	27 March 2017	Delayed due to the vetting audit (management request).
FS - Branch Network Sales Process	N. Kennett (K. Gilliland)	Q3	Q3/Q4	Draft Report	n/a				02/03/2017	09 March 2017	27 March 2017	Unable to complete site visits in December due to operational reasons.
Financial Controls Framework Programme - Independent Testing	A. Cameron	Q3/Q4	Q3/Q4	Fieldwork (3 of 4 stages complete)	n/a				27/04/2017	04 May 2017	18 May 2017	Audit to be completed over 4 phases. PwC co-source arrangement.
FS - Branch Network Sales Quality Assurance Process	N. Kennett	Q4		Draft Report	n/a				27/04/2017	04 May 2017	18 May 2017	
Network Branch Service Centre - Handling of Agents Queries and Complaints	K. Gilliland (A. Cameron)	Q3	Q4	Draft Report	n/a				27/04/2017	04 May 2017	18 May 2017	
IT Controls Framework (Advisory) (Addition)	R. Houghton	Q3		Fieldwork	n/a					FY 2017/18	FY 2017/18	Replaced IT & Operations Governance - agreed with CIO to provide advisory work and ongoing assurance on design of new control framework
IT Security Transformation (Advisory) (Addition)	R. Houghton	Q4		Fieldwork	n/a					FY 2017/18	FY 2017/18	Replaced IT 3rd Party Management - agreed with CIO to provide advisory work and ongoing assurance on Security Transformation project.
Business Continuity and Crisis Management - PO	K.Gilliland (J. MacLeod)	Q3	2017/18	Postponed to 2017/18						FY 2017/18	FY 2017/18	Replaced with DC Pensions / Vetting audit. Will test BC in 2017/18.
Procurement Process	A. Cameron	Q4	2017/18	Postponed to 2017/18						FY 2017/18	FY 2017/18	New Head of Procurement currenlty reviewing processes. Postpone the review to 2017/18.
IT & Operations Governance and IT Risk Management	A. Cameron	Q3	2017/18	Postponed. Replaced with IT Controls Framework Advisory								Postponed to 2017/18 to allow new IT Control Framework to be designed, implmented and embedded.
IT Third Party Management	A. Cameron	Q4		Merged with BTA. Replaced with IT Secu-rity Transformation								Cancelled as the BTA covered 5 most significant IT 3rd Party contracts as part of the Third Party Vendor Management review.

[1] Following further review and discussion with the CIO (Rob Houghton) it was agreed to update the rating for the IT DR report from Average to Adverse

POL00401624

Appendix 2a

INTERNAL AUDIT EXECUTIVE SUMMARY: Identity and Access Management

Ref. 2016/17-01

GE Sponsors: Jane MacLeod - Group LRG Director; Al Cameron – Group CFO; Rob Houghton – Group CIO; Martin Kirke – Group HR Director

Adverse

1. Background

Identity and Access Management (IAM) is the security and business framework (policies, procedures and processes) which enables the right individuals to access the right resources at the right times for the right reasons, preventing inappropriate access to information.

2. Audit Objective and Scope

Significant internal control weaknesses have been raised (by external and internal auditors) in recent years over Post Office's Identity and Access Management (including joiners, movers, leavers' (JML) access rights). This review evaluated the current status of the overall identity and access management process and more specifically the joiners, movers, leavers' access management processes and the associated controls.

It was not within the scope of this audit to review access rights to individual applications.

3. Key Observations

This audit identified major weakness in the following areas:

1. Process Governance

- Lack of overall IAM governance (e.g. no ownership of the end to end process, no process diagram).
- IAM–JML access management responsibilities (RACI) and controls are not clearly and transparently defined.

2. People training and awareness

- Line managers not well informed about their responsibilities regarding IAM -JML process.

3. Joiners, movers, leavers' processes and controls

- No assurance that access rights are limited to a need to know basis.
- HR does not have a full overview of all parties working for PO (employees, contractors). Additionally there is no overview of 3rd parties (suppliers) accessing PO data /systems.
- No assurance that access rights are reviewed when someone moves role/function.
- Periodical access reviews not in place (for LAN, share drives and all applications).
- No assurance that leavers' access rights are removed (timely).
- Data and system owners have not been identified (responsibilities assigned).
- Non-compliance with the access control standard/policy.

POL00401624

Appendix 2a

INTERNAL AUDIT EXECUTIVE SUMMARY: Identity and Access Management

Ref. 2016/17-01

4. Conclusion

This report has been rated **Adverse** as in our opinion IAM (Joiners, Movers, Leavers' access rights) requires immediate management attention to improve control to a satisfactory level of maturity.

A fundamental gap in the IAM process is the lack of overall governance. Currently the IAM and the joiners, movers, leavers' (JML) processes are run in silos by the functions involved (HR, line managers, IT) without any oversight or ownership of the end to end process to ensure controls are effective and information is accessed only on a need to know/have basis. Furthermore the lack of clear data and system owners puts the responsibility for ensuring adequate access to information with the line managers. Additionally there are no mechanisms in place to ensure such accesses have been granted appropriately and removed on a timely basis.

The issues raised in this report are not new as they have been raised previously by external and internal auditors and insufficient progress has been made to mitigate the risks linked to inappropriate access to information. An effective IAM is also part of the basic controls of cyber security.

5. Management Response

The findings from this audit demonstrate that Post Office has some way to go to define its approach to data and embed appropriate controls around access to Post Office's systems and the resulting access to, and use of, data. It has been agreed by the GE sponsors of this audit that the LRG Director will take overall accountability for the end to end IAM process which will have dependencies on HR, Operations and IT. A working group will be set-up to design what a good IAM/JML process looks like end to end, followed by a gap analysis comparing the design with the current processes and an implementation plan which will seek to embed controls and a self-assessment regime into the final processes.

- Jane MacLeod (Group LRG Director) -

POL00401624

Appendix 2b

INTERNAL AUDIT EXECUTIVE SUMMARY: BTA – Business Case Development

GE Sponsor: Alisdair Cameron (Chief Finance and Operating Officer)

Satisfactory (with exceptions)

1. Background

Previous Business Transformation Assurance reviews have highlighted a key risk theme regarding the inconsistency in overall quality of business cases, lack of detail within the business cases submitted, and issues have been raised related to business cases' financial management and reporting. During 2016 Post Office deployed a new change methodology, "One Best Way" to provide improved governance over change projects and programmes.

2. Audit Objective and Scope

The objective of this review was to give an independent view of the effectiveness of the business case development process in place across Post Office Limited (POL), which is governed by the One Best Way (OBW) methodology. The following aspects have bene assessed: consistency of application of the OBW transformation methodology (covering the quality and content of business cases), clear and robust documentation to support assumptions, and that it is appropriately reviewed.

The review focused on a sample of four programmes across the transformation programme, chosen randomly: IT Networks, Paddington, HR Transformation and Branch Information Improvement.

3. Key Observations

Overall, the application of the OBW methodology has led to an improvement in the quality of business cases submitted and no significant instances of non-compliance with the framework were identified.

However, some further improvements have been identified related to the framework and associated guidance, particularly in ensuring business cases provide a comprehensive representation of the change programmes' aims and its associated costs and benefits; as well as a need to track budgetary approvals more effectively.

4. Conclusion

We have rated this report **Satisfactory (with exceptions)** as the identified improvements would strengthen the internal controls around business development cases, cost and benefits tracking.

5. Management Response

"To confirm I am happy with the review and the findings identified. It is good to note that the application of the OBW methodology has led to an improvement in the quality of business cases submitted, and no significant instances of non-compliance with the framework were identified. The recommendations within the report and the agreed actions will further strengthen our approach and control of the delivery in line with the business case."

Angela Van Den Bogerd (People and Change Director)

POL00401624

7.1 Modern Slavery Act

Authors: Jim Carter and Kelly Taylor Sponsor: Martin Kirke Meeting date: 4 May 2017

Executive Summary

Context

The Modern Slavery Act 2015 (the Act) challenges slavery, domestic servitude, forced and compulsory labour and human trafficking. Post Office is required to produce an annual slavery and human trafficking statement (Statement) setting out what steps have been taken to ensure its business and supply chains are slavery free. This paper attaches the second Statement which documents progress on our previous year's commitments and outlines the actions that we are committed to taking this year 2017 -18. This must be approved by the Post Office Board and signed by a Director.

Questions this paper addresses

1. What specific risks should the board be aware of?
2. What are other businesses doing and how do we compare?
3. What action have we taken so far and in particular what progress have we made with regards to our commitments contained in our 2016 MSA Statement?
4. What commitments are the Steering Group recommending we make for 2017?

Conclusion

- Post Office has been undertaking due diligence on its business and supply chains to identify any risk areas.
- Post Office has prepared a revised Statement in line with the legislation which must be published within 6 months of year end.
- A steering group was appointed in January 2016 is responsible for proposing actions, creating relevant project plans and continuing to develop and monitor our approach to MSA legislation.
- The steering group has identified that the highest level of risk is within our Agency network. We have already begun to take action to address this risk including amending our contracts with our Postmasters to require compliance with the Act.
- The first Post Office's MSA Statement was prepared using Home Office guidance and in consideration of other available Statements by UK and international companies.

POL00401624

- The nature of the legislation allows for the organisation to build a robust approach to the MSA over time. Our MSA statement, therefore, requires updating every twelve months and will outline progress on previous commitments and actions we are taking in the next twelve months.

Input Sought

The RCC and GE are asked to approve the 2017/18 statement and endorse actions for the business to take forward this financial year.

POL00401624

The Report

What specific risks should the board be aware of?

The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36,000,000. It will therefore not apply directly to Postmasters if their turnover is less than £36 million per year.

However, Postmasters are part of the Post Office supply chain. Post Office must state what steps it has taken to ensure that slavery and human trafficking is not taking place in any of its supply chains or in any part of its business.

The due diligence that we have undertaken so far indicates that there is a potential risk of non-compliance within our agency Network. The reason for this is that there are a large number of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS. They work directly for the Postmasters (including multiple partners). We have already taken action to begin to address this risk including reviewing our contracts with our Postmasters to require compliance with the Act.

What are other businesses doing and how do we compare?

We looked at statements for international companies with complex supply chains to get a flavour for content and examples of initiatives.

Many companies have not yet published their Statements, but we have looked at a variety to ensure that our approach is consistent. By way of an example, Ford have published a statement which is approximately two pages long. They recognise their supply chain is extensive and complicated and that it presents challenges. Some of Ford's initiatives are similar to ours - this is encouraging given that Post Office's business and supply chains are not as extensive as Ford.

We also looked at what some of our partners are doing:

WH Smiths

- Statement not yet published.
- They use the Ethical Trading Code of Conduct and Human Rights Policy. It incorporates the ILO Conventions to scope out the current position on Modern Slavery related matters.
- The policy specifies a person who takes responsibility for the Code.

Bank of Ireland

- Do not currently have a Modern Slavery statement.

POL00401624

- Publish a Responsible Business Report which currently makes no reference to Modern Slavery.
- As a key partner, Post Office should investigate directly with BOI as there appears to be very little in terms of Modern Slavery related matters.

We are confident that the detail in our Statement, our commitments documented last year and our proposed actions for this year are appropriate at this stage. We will monitor developments, however, and keep the adequacy of the Statement under review.

What action have we taken so far?

Responsibility for our Modern Slavery initiative was handed to a steering group lead by Hannah Dalton (Head of HR). The steering group was appointed in January 2016. The group is now led by Jim Carter and Kelly Taylor.

Since 2016 we have been required under the legislation to publish a Modern Slavery Statement. This documents what actions we will be taking for the following year with regards to MSA. In 2016 we made three specific commitments and progress on these commitments is outlined below:

Commitments from 2016 Statement	Progress on 2016 commitments
Updating Postmaster's selection and appointment process to address MSA requirements	We have now reviewed the Postmaster's contract and believe that ii is robust enough to cover the MSA legislation. We have also supplemented the contract process with a set of Guidelines for Postmasters (Appendix 1)
Amending our standard form procurement contracts.	We have reviewed our standard form procurement contracts and believe that our 'applicable laws' clause covers POL for breaches of MSA. Our PQQ process has also been amended to take account of MSA and suppliers must confirm that they comply with their obligations under the MSA and provide a copy of their MSA Statement.
Developing a communication and training plan to ensure our suppliers, staff and agents are aware of Post Office's obligations in relation to Modern Slaver and informing them about the Modern Slavery Helpline.	We have now produced a communication plan for roll out in 2017, (Appendix 2). The MSA is also now referenced in our Whistleblowing Policy (Appendix 3) and will be added to our Code of Business Standards, which is currently being redrafted.

POL00401624

	A training plan remains under development. This year, however, our commitments are focussed on raising awareness. The Steering Group anticipate the training requirement to increase as we move towards 2018 as we begin to build a suitable due diligence and compliance capability.

What commitments are the Steering Group recommending we make for 2017?

The Steering Group has now agreed upon a proposed series of commitments for 2017. The focus for 2017 will be on increasing awareness and understanding across POL of the MSA.

- Roll out our MSA Communication Plan
- Review our approach to audit and compliance and make recommendations around a suitable regime to take forward.
- In the light of the recommendations from our review of audit and compliance, to develop a relevant Training Plan.

POL00401624

Post Office Limited (Post Office) & Post Office Management Services Limited (POMS)
Modern Slavery Transparency Statement 2017-18
May 2017

Executive Summary
This statement sets out the steps we have taken during the last financial year to ensure that Modern Slavery is not taking place in any of our supply chains or any part of our business. It is made pursuant to section 54(1) of the Modern Slavery Act 2015 (MSA). The Statement also sets out our commitments for the next twelve months with regards to the legislation.

Our business
Post Office is the UK's largest retail network and the largest financial services chain in the UK with more branches than all of the UK's banks and building societies put together. We have provided services for more than 370 years and currently supply more than 170 products and services (mails & retail; financial services; governments services; and telephony) from a Network of more than 11,500 Post Office branches nationwide.

Post Office directly manages currently over 300 of the Network branches. The remainder of the branches are managed on an agency basis by Postmasters and multiple partners.

Our supply chains
We currently operate throughout the UK, however our supply chains connect with suppliers with a global reach.

Banking services
Our banking services are provided through a joint venture with the Bank of Ireland (BoI).

Postmasters
Postmasters can operate one or more branches. As agents they have control on how they run their branches on a day-to-day basis. All those working in an agency Post Office branch are employees of the Postmaster.

Multiple partners
A large proportion of the agency part of our network is run by multiple partners.

Trade Unions
In our directly managed branch network, we work closely with the Communications Workers Union (CWU) and Unite (CMA) Communications Managers Association.

Third Party Suppliers/Procurement
We also procure products and services from a wide range of national and international businesses.

Responsibility and due diligence
Responsibility for our Modern Slavery initiatives currently resides with a steering group which was appointed in January 2016. It is tasked with the development of a project plan to carry out due diligence and implement change.

Where are the risks of Modern Slavery at Post Office/POMS?
The due diligence that we have undertaken so far indicates that there could be a risk of non-compliance within our agency network because there are a large number of people employed by Postmasters (including multiple partners) but who are not employees of Post Office or POMS.

POL00401624

They work directly for the Postmasters (including multiple partners). We will be taking action to address this risk (see below).

What we have done so far

- Our Whistleblowing Policy has been updated to include references to concerns about Modern Slavery.
- Our Code of Business Standards will reference the issue of Modern Slavery.
- We have adapted the Post Office recruitment policy to address MSA requirements.
- We conducted an assessment of the Post Office procurement process to ensure it aligns with the MSA. As part of this process we have conducted a review of the criteria used by Post Office to evaluate whether suppliers meet Post Office's minimum tendering requirements. As a result of this we have now reviewed our standard form procurement contracts to ensure that they cover POL with regards to the MSA legislation.
- Our PQQ process has also been amended to take account of MSA. Suppliers must now confirm that they comply with our MSA Statement.
- We have reviewed the Postmaster Contract of Engagement and have written Guidelines for Postmasters to assist them in complying with MSA legislation.

Next steps

Throughout 2017 we will be committed to a programme of 'Building Awareness'. This includes:

- Rolling out our MSA Communication Plan across all of POL, including our directly employed colleagues, postmasters and supply chain.
- Reviewing our approach to audit and compliance and make recommendations around a suitable regime to take forward.
- In the light of the recommendations from the review of audit and compliance, to develop a relevant Training Plan in support of any proposed new regime.

Our policies

We currently operate the following policies that describe our approach to Modern Slavery:

- *Code of Business Standards*
- *Whistleblowing Policy*

Further information

If you have any concerns about the issues raised in this statement or if you think you have identified signs of Modern Slavery then please either contact us or call the Government's Modern Slavery Helpline on 0800 0121 700.

Signed: .....
Name: .....
Position: .....
Date: .....

POL00401624

Appendix 1

Modern Slavery Act 2015

Guidance and Contractual Standards for Postmasters.

1. WHY DO I NEED TO KNOW ABOUT THIS?

1.1 The Modern Slavery Act describes a number of offences which will constitute modern slavery. For example, it makes it an offence for any person, irrespective of whether they have a Post Office, or any other kind of business, or are acting in a purely personal or domestic capacity

a) to hold another person in slavery or servitude in circumstances where the person knows or ought to know that the other person is held in slavery or servitude; or
b) to require another person to perform forced or compulsory labor in circumstances where the person knows or ought to know that the other person is being required to perform forced or compulsory labor; or
c) to arrange or facilitate the travel of another person with a view to that person being exploited.

1.2 Indicators of forced labour would include:

- Abuse of vulnerability
- Deception
- Restriction of movement
- Isolation
- Physical and sexual violence
- Intimidation and threats
- Retention of identity documents
- Withholding of wages
- Debt bondage
- Abusive working and living conditions
- Excessive overtime

1.3 The Act ensures that perpetrators of modern slavery can be given suitably severe punishments for modern slavery crimes, including life sentences.

1.4 The Act applies to you and you have a personal legal obligation to comply with it.

2. PURPOSE OF THIS GUIDE

2.1 This Guide does not give an overview of the Act but it does explain Post Office Limited's contractual standards on modern slavery. These instructions have contractual effect.

Feb 2017

POL00401624

2.2 Post Office's contractual standards apply to all Postmasters, including sub-postmasters, franchisees, operators and any other agents operating Post Office branches or outreach services.

2.3 Compliance with these standards does not of itself ensure compliance with the Modern Slavery Act. It remains the responsibility of Postmasters to ensure they comply with the Act.

2.4 We are committed to ensuring no one suffers any detrimental treatment as a result of reporting in good faith their suspicion that modern slavery of whatever form is or may be taking place in any part of our business, including in a Post Office branch or any retail business associated with it, or in any of our supply chains. Detrimental treatment includes contract termination, corrective action, threats or other unfavourable treatment connected with raising a concern. However, if a postmaster has been involved in any breach of the Act or these standards, we may take corrective action against him/her, which may include contract termination. Individuals that have concerns about modern slavery practices will be able to notify Post Office by contacting the Network Business Support Centre (NBSC) or Grapevine.

2.5 Post Office Limited may amend this Guide and the contractual standards at any time.

3. POST OFFICE CONTRACTUAL STANDARDS

3.1 You must ensure that you read, understand and comply with this Guide and the Modern Slavery Act 2015. Further information regarding the Act can be sourced from the Government's website gov.uk

3.2 You are responsible for the prevention, detection and reporting of modern slavery in any part of your Post Office branch and any associated retail business or supply chains.

3.3 You must notify Post Office Limited as soon as possible if you believe or suspect that a breach of, or conflict with the Act has occurred, or may occur in the future. You must do this in the following by contacting the Network Business Support Centre.

3.4 You should raise any concerns you have about any issue or suspicion of modern slavery in any parts of your or our business or supply chain at the earliest possible stage.

3.5 You should report it to us even if you are unsure about whether a particular act, the treatment of workers more generally, or their working conditions within any tier of your or our business and/or your or our supply chains constitutes modern slavery.

3.6 We aim to encourage openness and will support anyone who raises genuine concerns in good faith in relation to modern slavery, even if they turn out to be mistaken.

4. FAILURE TO MEET THE CONTRACTUAL STANDARDS

4.1 Any Postmaster who fails to comply with these contractual standards and/or the Modern Slavery Act 2015 is at risk of contractual action, including possible immediate contract termination.

Feb 2017

POL00401624

Appendix 2

Proposed MSA Communication Plan

When	Who	What	How
	all	Policy statement on intranet	intranet
	L300	headline - link to policy statement	direct email
	Central team colleagues	headline - link to policy statement	one focus email
	Supply Chain	headline - link to policy statement	one focus email
	Branch teams - DMB	headline - link to policy statement	one focus email
	Branch teams - agents	headline - link to policy statement	branchfocus email
	all	reminder where to find info	One/intranet
	Branches - DMB	"what this means to you"	one focus email
	Branches - agency	"what this means to you"	branchfocus email
	Central teams	"what this means to you"	one focus email
	all	reminder	One/intranet
	Branches - DMB	how to report	one focus email
	Branches - agency	how to report	branchfocus email
	Central teams	how to report	one focus email
	all	reminder	One/intranet

POL00401624

Appendix 3

Quote from POL Whistleblowing Policy.

What is Whistleblowing

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or externally, for example to a regulator. The law on Whistleblowing is contained in the Employment Rights Act 1996 as amended by the Public Interest Disclosure Act 1998. Wrongdoing includes criminal activity, civil offences (including negligence, breach of contract, breach of administrative law), miscarriages of justice, dangers to health and safety or to the environment and the cover up of any of these.

Workers should raise a concern if they are aware of, or suspect, wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). Some examples (this is a non-exhaustive list) of situations where a worker may raise a concern are:

- Financial Crime including Fraud, Money Laundering and financing of terrorism, Bribery and Corruption,
- Giving, offering or taking of bribes,
- Financial mismanagement,
- Misreporting,
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures (including the Code of Business Standards),
- Concerns about slavery or human trafficking, and
- Any conduct likely to damage Post Office's reputation.

A Whistleblower is a person who raises a genuine concern relating to any wrongdoing including any of the above. If a worker has any genuine concerns related to suspected wrongdoing, they should report it under this Policy.

If a worker is uncertain about whether something is within the scope of this Policy, they should seek advice from the Whistleblowing Officer, whose contact details are set out in this Policy.

(Extract from Section B. Context)

POL00401624

8.1) Horizon Scanning Report

Author: Jane MacLeod

Meeting date: 4 May 2017

Executive Summary

Context

As part of its remit, the Risk & Compliance Committee should consider legal, regulatory and other external developments on behalf of Post Office in order to ensure that impacts on Post Office (including its customers, staff, suppliers and stakeholders) are understood and being appropriately managed. This report highlights current developments of relevance to Post Office and the work that is being done to monitor these.

Questions this paper addresses

1. What are the material legal, regulatory and other external risks the Post Office executive and Board should currently be aware of?
2. What work is being undertaken to assess, monitor and mitigate these risks?
3. Who is accountable for this work and how will it be reported through Post Office governance structures?

Conclusion

1. There are a number of material developments which either will or could impact Post Office and details of these are set out in this summary.
2. In each case, work is being undertaken to monitor and assess the risks arising from these developments. The Legal, Risk & Governance team is working with the different stakeholders to progress this assessment.
3. Governance structures and reporting lines will be developed to ensure there is appropriate representation from across Post Office in formulating responses to, and mitigation plans for, these developments.
4. The status of those developments which have previously been noted to the Committee are set out in the Appendix.

Input Sought

The R&CC is asked to note these developments.

POL00401624

The Report

Corporate Governance: House of Commons BEIS Select Committee Report

1. Following the publication of the Government's Green paper on Corporate Governance in November 2016, details of which were provided to the RCC for its meeting of 11 January 2017, the House Of Commons BEIS Select Committee published its own report on Corporate Governance on 5 April 2017.

2. The Committee's report is largely focused on large private-owned, listed, companies and, therefore, many of its recommendations are not applicable to Post Office directly. However, given this policy area lies with BEIS, our shareholder, it is reasonable to assume that there will be an expectation that the Post Office will take steps to follow best practice. As a matter of fact, Post office is reasonably well placed in terms of its approach to Corporate Governance generally and we do not, currently, foresee any particularly tricky challenges arising from this work.

3. However, one particular area which will require some consideration and potential future changes to existing Post Office practice relates to Executive Pay generally and to Long Term Financial Incentives, or LTIPs, in particular. The Committee recommends that LTIPs be discontinued as soon as possible, as a means of promoting responsible decision making by executives in the long term interests of their companies.

4. Instead, the report recommends that, following consultations with stakeholders, the UK Corporate Code of Conduct should be amended to establish deferred stock, rather than LTIPs, as best practice in incentivising long term decision making. Although our LTIP system models (current) good practice in this area, a shift away from this system to one based on deferred stock present the Post Office with a self-evident in that we do not have stock to allocate to this, or indeed, any other purpose.

5. Nonetheless, the Remuneration Committee will need to consider the implications of this broader shift away from LTIPs and POL Management will bring forward some suggestions and recommendations to one of its future meetings, to see what we might be in a position to do to give effect to the spirit of this shift, within the constraints of our ownership model.

POL00401624

General Election 8 June

6. The Committee should be aware that, with the general election having been called for 8 June, and purdah rules already being in effect, it is highly likely that delays will be experienced in the agreement and publication of a number of legislative and regulatory measures which may have an impact on the Post Office. This will, for instance, be the case in relation to the rules implementing the Enterprise Act 2016, including the rules of the taxation of redundancy payments. Colleagues across the business will be keep a weather eye out for developments in their respective areas.

STATUS OF PREVIOUSLY REPORTED DEVELOPMENTS

Issue	Brief Description	Update
Brexit	Assessing impact on Post Office following the result of the Referendum	No new developments to report at this juncture.
GDPR	New and more onerous EU Data Protection Regulation	Programme now properly underway, with the technical data mapping exercise being prioritised to unlock workstreams.
Networks and Information Security Directive	New EU Directive to support GDPR	
Modern Slavery Act 2015	A slavery and human trafficking statement must be prepared and published each year setting out what steps have been taken to ensure modern slavery is not taking place in the business or its supply chains.	MSA statement is table for consideration and agreement at this meeting.

POL00401624

Company no. 8459718 – Strictly Confidential

RCC 17/11 – 17/20

POST OFFICE MANAGEMENT SERVICES LIMITED (Company)
RISK, COMPLIANCE AND CONDUCT COMMITTEE (RCCC)
(A committee of the Executive)

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 22 February 2017 at 13.30 pm

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Gerry Barrett (GB)	Head of General Insurance
	Stephen Gaines (SG)	POMS Compliance Manager
	Russell Tavener (RT)	Head of Commercial Operations
	Michael Brown (MB)	Deputy for Head of Commercial
	Gill Craig (GC)	Deputy for Head of Travel
	Emma McGinn (EMG)	ISAG Representative
In Attendance:	Ann Young (AY)	Compliance Advisor
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Sanjeeve Thakrar (ST)	Risk Manager
	David Williamson (DW)	Design Authority
Apologies:	Ben Foat (BF)	Head of Legal
	Ryan Griffin (RG)	Head of Protection

RCC17/11 WELCOME, QUORUM AND CONFLICTS OF INTEREST

The Chairman declared the meeting quorate and open.

RCC17/12 MINUTES OF THE MEETING HELD ON 24 JANUARY 2017

The minutes of the meeting held on 24 January 2017 were approved and the Chairman was authorised to sign them as a true record of the meeting.

RCC17/13 MATTERS ARISING AND ACTIONS LIST

(a) **Action RCC 16/45 (c)** –. With the changes in ISAG, RT is to have a meeting to see where this is currently sitting. Ongoing

(b) **Action RCC 16/92 (b)** Control Self Assessment Contract is awaiting signature Ongoing

(c) **Action 16/113 (a)** Multi AR Agreement SH to discuss with Ben Foat Ongoing

(d) **Action 16/114 (d** Aviva Complaints - SH and Tom Bermingham are to arrange a call with Aviva. Ongoing

(e) **Action 16/115 (e)** SH to discuss the complaint reporting process with Angela Van Bogerd. Ongoing

POL00401624

(f) **Action 17/4 (a)** Risk Acceptances ST to provide a list of new risks which will be circulated to the meeting in advance. Closed

(g) **Action 17/5 (a)** SH to provide an update of funds from POMS- Colin Newton to formulate a procedure - Ongoing

(h) **Action 17/6 (a)** Webhelp consistent 95% pass rate MB to discuss with Webhelp - Ongoing

(i) **Action 17/6 (c)** Panel of insurers supplied by Cunningham Lyndsay UK Ltd. GB to present to Prodco next month - Ongoing

(j) **Action 17/6 (e)** Business insurance MI is now being received – Closed

(k) **Action 17/6 (f)** GB to interrogate the cancellation reasons on report supplied by Junction – Ongoing

(l) **Action 17/6 (g)** MB to listen to a sample of EOD to confirm not complaints. Closed

(m) **Action 17/6 (h)** MB to attend a meeting at Junction to obtain more information on complaints. Closed

(n) **Action 17/6 (i)** MB to investigate the 47% upheld rate at Collinsons – Ongoing

(o) **Action 17/7 (a)** EMM to raise an incident on the pause and resume function- Ongoing

(p) **Action 17/7 (b)** EMM checked the feedback is provided to staff. Closed

(q) **Action 17/7 (f)** Compliance Review recommendation have been forwarded to relevant owner – Closed

(r) **Action 17/9 (a)** FS consultation period and FS behaviour – Closed

(s) **Action 17/9 (d)** Royal London call validation- Closed

POL00401624

RCC17/14 **RISK MANAGEMENT**

(a) ST confirmed that Project Zeus is the highest risk on the Risk Register. DW has confirmed that the system will go live on 5 March with the defects in the system known. System issues will be prioritised, these will include testing, and dependency work round

(b) Project Hermes (2nd Phase of Zeus is due for completion on 1 April. This will include the FCA requirement on renewals

Action ST (c) TIF remains high risk and RT expressed concerns on TIF ability to handle claims especially if TIF is extended to Money Supermarket. ST is to review and amend the risk score if required.

Action ST (d) ST confirmed that the risk relating to Marketing and the proposed restructure. will increase the risk score to reflect the lack of marketing capability

(e) ISAG resource was discussed. EMG confirmed that there is a meeting booked for 23 Feb to discuss the options available for ISAG

(f) EMG confirmed that her last day at the Post Office will be 13 April 2017

RCC17/15 **INCIDENT MANAGEMENT**

(a) ST confirmed that there are a number of incident relating to Junction on the Incident Register. ST has spoken to both BT and GB who have confirmed that Junction have been unable to provide updates for these incidents

(b) SH confirmed that there have been more incident of the inactive travel discount code being used in Branches. SH has asked Ben Trigg to chase Horizon for a fix for this issue.

(c) SH confirmed that a company called Aviva Protects had contacted customer who had taken a policy with Post Office to change to their policy. It is not clear if the data leakage is at the Post Office or Aviva as no source has been identified.

(d) There have been three incident in which a life policy has been sold where the life assured was not present. These are to be added to the Risk Register.

RCC17/16 **1st LINE COMPLIANCE REPORT**

(a) MB discussed Conduct Risk Scorecard and noted that Complaints for the period were slightly up. This was thought to be due to seasonality.

(b) MB confirmed that the Webhelp QA red calls had increased to 15% this month. This is due to the new agents who have recently be trained. Feedback has been provided and the February figures will be checked for improvement.

(c) POMS is now receiving the results of the Success Factors mandatory modules. These results will be added to the Conduct Risk Scorecard.

POL00401624

(d) MB confirmed that he is in discussion with Collinson regarding their high upheld rate (**Action 17/6 (i)).**

Action MB (e) MB will be contacting Kenny and Craig at Webhelp to discuss complaints where incorrect information is provided on policy or policy information is not provided to the customer.

Action RT (f) RT is to follow up with Junction on the procedure for dealing with verbal complaints.

RCC17/17 **2ND LINE COMPLIANCE REPORT**

(a) EMM presented the 2nd line Travel compliance report. EMM confirmed that there had been an increase of 31 variances identified. (New Sales 13, Renewal 14 and Cancellations 4) The report identifies that there were several different reasons for the variances.

(b) EMM also identified that there were instances where there was no screen capture for travel but this has been fixed for the go live date for project Hera.

Action EMM (c) EMM identified an issue that the red calls were not being fed back in a timely manner. EMM has asked for an incident to be raised

(d) AY confirmed that the VMS monitoring had been undertaken, Including reviews of CRM. In total 4 calls had been reviewed. There was 1 variance identified in one of the CRM calls. One instance in the CRM calls the CRM advised that the customer was covered immediately on an Over 50 plan and One variance on the FS call in which it was not explained that the first quote was an indicative quote.

(e) AY confirmed this the February data will be the last month that FS VMS call will be available. There will be an increase in the number of CRM VMS calls reviewed in future months.

(f) AY confirmed that outstanding Compliance Review Recommendations have been forwarded to relevant owners and responses are now being received

Action SH (g) SH confirmed that Compliance Monitoring Officers will be providing a report on the finding from the reviews undertaken for the next RCCC in March.

(h) SH confirmed that due to the delay of project Zeus, it has been decided to delay the New Business review and MTA review to later in the year.

POL00401624

(i) A report was provided on the Financial Promotions received into POMS for January. The report focused on what Department were submitting the Financial Promotions and the quantities received. The Report also covered how many of the Financial Promotions were approved on the first submission and how many had to be re-submitted.

RCC17/18 **ISAG REPORT**

(a) EMG provided an ISAG report to cover January and February. The following projects were covered

- Zeus Accenture
- Zeus Hexware
- POMS / PO SMP
- Top Suppliers
- ISMS
- House Position
- BIA/PIA/PCI-IA

(b) EMG highlighted the following risks

- People using own devices to store POMS data.
- Email from Richard X James on 13 January 2017:
  "As part of the Zeus implementation, we are removing the need for Webhelp to store the full client record.

Action ST © EMG confirmed that ISAG had not been informed of any POMS incidents. ST agreed to provide ISAG with a Nil return if no incidents are receive into POMS.

Action EMM & RT (d) EMG confirmed ISAG Data Protection Team receive a number of customer queries into their Mailbox each month regarding Travel Insurance. EMM confirmed that these emails are sent to her. RT to check the outbound contact.

RCC17/19 **POL REPORT**

(a) David Williamson (DW) joined the meeting to present the new MI suite for POMS. The MI suite will build on evidence on behaviours in our sales channels. DW provided screen of cancellations which showed graphs of the different channels and the cancellations and the periods in which the cancellations occurred.

DW confirmed that complaints and renewal information will also be included going forward

DW welcomed feedback on the report and any suggestions for improvement

POL00401624

ANY OTHER BUSINESS

RCC17/20

There was no other business raised. There being no further business the meeting was closed.

The next meeting of the RCC would be held on 23 March 2017 at 14.00pm.

…….. ……

Chairman **Date**

POL00401624

RCC 17/21 – 17/30

POST OFFICE MANAGEMENT SERVICES LIMITED (Company)
RISK, COMPLIANCE AND CONDUCT COMMITTEE (RCCC)
(A committee of the Executive)

Minutes of an RCCC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 23 March 2017 at 14.00 pm

Present:	Susie Hayward (SH)	Head of Risk and Compliance (Chairman)
	Gerry Barrett (GB)	Head of General Insurance
	Stephen Gaines (SG)	POMS Compliance Manager
	Russell Tavener (RT)	Head of Commercial Operations
	Michael Brown (MB)	Deputy for Head of Commercial
	John Brinsden (JB)	Deputy for Head of Protection
In Attendance:	Ann Young (AY)	Compliance Advisor
Apologies:	Ben Foat (BF)	Head of Legal
	Ryan Griffin (RG)	Head of Protection
	Gill Craig (GC)	Deputy for Head of Travel
	Emma McGinn (EMG)	ISAG Representative
	Elizabeth McMenemy (EMM)	Compliance Advisor
	Sanjeeve Thakrar (ST)	Risk Manager

RCC17/21 WELCOME, QUORUM AND CONFLICTS OF INTEREST

The Chairman declared the meeting quorate and open.

RCC17/22 MINUTES OF THE MEETING HELD ON 20 FEBRUARY 2017

Action SH (a) The minutes of the meeting held on 20 February 2017 were reviewed. SH confirmed there was a few minor amendments to make and would forward these to AY for inclusion. It was agreed the action points arising from the minutes would in future be sent to all participants one week prior to the next Risk and Compliance Conduct Meeting.

RCC17/23 MATTERS ARISING AND ACTIONS LIST

(a) **Action RCC 16/45 (c)** –. With the changes in ISAG, RT is to arrange a meeting with the relevant individuals to discuss POMS PCI requirements following the decision for POMS to have a separate contract with Globalpay. Ongoing

(b) **Action RCC 16/92 (b)** Control Self Assessment will follow after Xactium is in place Postponed until June 2017 Ongoing

(c) **Action 16/113 (a)** Multi AR Agreement SH to discuss actions with Ben Foat Ongoing

POL00401624

(d) **Action 16/114 (d** Aviva Complaints - Increase in volume discussed with AVIVA. POMS are satisfied the correct diagnostics are taking place in AVIVA before referral to BOI and WebHelp. Closed

(e) **Action 16/115 (e)** Angela VDB has moved to another role. Complaints process will be subject to regular review. Close

(f) **Action 17/5 (a)** Jane McLeod has documented a new procedure for the management of intercompany funds transfers- Closed

(g) **Action 17/6 (a)** Webhelp consistent 95% pass rate Discussion held with EMM who validated the consistency of WebHelp Quality Score due to the scrutiny of 2nd line checks undertaken to which variances were limited. – Closed

(h) **Action 17/6 (c)** Home claims to be managed by Cunningham Lyndsay UK Ltd. GB to provide update next month - Ongoing

(i) **Action 17/6 (f)** GB to interrogate the cancellation reasons on report supplied by Junction – Closed

(j) **Action 17/6 (i)** MB to investigate the 47% upheld rate at Collinsons – The high upheld rate will be validated as part of the complaints review. Closed

(k) **Action 17/7 (a)** EMM to raise an incident on the pause and resume function- Closed

(l) **Action 17/14 (c)** TIF claim handling ST to review and amend risk score if required Closed

(m) **Action 17/14 (d)** ST to review and amend the risk score to reflect the lack of marketing capability Closed

(n) **Action 17/16 (e)** MB to contact Webhelp to discuss policy information on complaints. To pick up as part of complaints review. Closed

(o) **Action 17/16 (f)** RT to discuss verbal complaints procedure with Junction. To pick up as part of complaints review Closed

(p) **Action 17/17 (c)** EMM to raise an incident regarding feedback to agents when a call is scored red Ongoing

(q) **Action 17/17(g)** Compliance Monitoring to be supplied to the RCCC for April Ongoing

(r) **Action 17/18 (c)** ST to provide ISAG with nil return if no incidents are received into POMS Closed

(s) **Action 17/18 (d)** Incorrect email address – RT to check the outbound contact details for Travel Insurance Ongoing

POL00401624

RCC17/24 **RISK MANAGEMENT**

(a) SH confirmed that there have been 3 new risks accepted by ARC and the Board last week.

- Strategy of the business was considered outside of appetite, this is due to the income stretch in budget and has been discussed at Board level and now accepted.
- IPA staff resources were also considered outside of appetite. Jane McLeod has confirmed that new staff will commence 1st April and IPA will continue to provide resources to POMS.
- Staff resources and requirement to fill senior level positions and implement target operating model.

Action ST (b) GB confirmed that the increase in the BGL protected bonus rate had initially affected the retention rate but this has since recovered. This risk can now be closed on the risk register.

(c) SH confirmed that the Zeus project is now live with issues. The risk will need to be reviewed. SH also confirmed that the migration of the existing book will now take place on 8/9 April. Currently the call centre is running both systems.

Action ST (d) It was now considered that the Webhelp staff capacity issues had now passed and this risk can now be closed

Action ST (e) Hera Day 2 risk requires a review to update the description and score. ST to review.

Action All (f) SH requested that all risk owners visit the risk register and filter and update their own risks

(g) SH confirmed that the contract for the Xactium risk management system has now been signed and design and integration is expected to be completed within 12 weeks. SH advised the meeting that Xactium will be able to manage incidents.

RCC 17/25 **INCIDENT MANAGEMENT**

(a) AY confirmed that POMS has been advised that there were two further incidents of life policies being sold without the life assured being present. AY to monitor with FSRisk

Action SH & RT (b) RT discussed the Hexaware reporting and auctioning of incidents and it was agreed that SH and RT will review the Hexaware incident management process to align with POMS process

POL00401624

RCC17/26 **1st LINE COMPLIANCE REPORT**

Action SG & SH (a) The conduct scorecard was discussed and it was agreed that a review is required to ensure that the tolerance levels and metrics are correct.

Action RT (b) Webhelp performance on complaints was discussed and it was noted that the complaints uphold rate of 31% was high and needed review to understand the reasons and actions being taken. The monthly WH root cause forum was discussed with concerns this is not delivering the right results and required help from POMS. The WH resources for Complaints and QA were discussed. SH and RT agreed another meeting with Webhelp to follow up the meeting in December would be useful.

Action RT (c) It was agreed that a review of complaints was required to include a review of the travel upheld rates within WH and Collinson, the branch complaint data and how this could be more effective, the definition and reporting of EOD and positive actions to reduce numbers. RT to consider scope and approach, SG to review the FCA data regarding complaints and upheld rate to establish benchmarking for POMS complaint data

Action SG

(d) The WH QA results were reviewed and discussed. The low tenure of staff was reflected in the high failure rates and challenged whether the training was effective. The travel failures continued for the med screening questions and the life failures were mixed representing inexperience in the agents.

(e) The cancellation report/lapse curve was reviewed and discussed. MB to ensure future reports are for the whole of the previous month.

Action RT (f) SH noted that the information on branch cancellations are not providing the cancellation reason or customer details. The branches would like more meaningful information. RT to check with Royal.London to provide more information on cancellation reasons and how we can improve data provided to POL.

Action GB (g) One of the categories for cancellation reasons for Car/Home & Commercial vehicle is “policy renewed”. GB is investigate and obtain an explanation of this category.

Action SG (h) SG to discuss with Webhelp the reasons for cancellation on travel insurance

(i) Claims report was reviewed with no concerns. GB noted the impact of Storm Doris to home insurance claims and increase in abandonment rate

RCC17/27 **2nd Line Compliance Report**

(a) SG provided the 2nd Line compliance report from regarding the monitoring of calls at Webhelp. There were 38 variances identified during the month many housekeeping issues. However only 2 variances were found to be relating to customer detriment. SG confirmed the report would be

POL00401624

amended to reflect. The quality of the QA being performed was discussed and the actions to follow up on failures. To be picked up with WH at next opportunity.

(b) SG confirmed that there were 7 complaints in which Webhelp had been unable to obtain the branch application from the Post Office This could have an effect on the outcome of the complaint

(c) AY confirmed that the VMS monitoring had been undertaken, There were only 5 CRM calls available for review and it had been communicated to POL this the level of VMS and MS were not representative of the sales and needed to be increased.. This has been raised with FSRisk to organise more life and home insurance calls

(d) AY advised the meeting that 2 of the CRM videos reviewed had several amber scores within the videos. This has been raised with FSRisk who had confirmed that the procedure was that any video which exceeds 70% amber marking would be recorded as a Red (Fail). FSRisk to discuss and confirm when this would come into effect

(e) The Financial Promotion report was reviewed. SH confirmed that there was an improvement in Financial Promotion being signed off in the first instance.

RCC 17/28 **ISAG REPORT**

(a) There was no ISAG report provided this month.

RCC 17/29 **POL REPORT**

(a) There was no POL report provided this month

RCC 17/30 **ANY OTHER BUSINESS**

(a) There was no other business raised. There being no further business the meeting was closed.

The next meeting of the RCC would be held on 27 April 2017 at 14.00pm.

Chairman…….. **Date** ……

POL00401624

8.3) Whistleblowing

Author: Jane MacLeod

Meeting date: 4 May 2017

Executive Summary

Context

Post Office has a Whistleblowing Policy (adopted in May 2016) which requires an annual report to the Risk & Compliance Committee and the ARC on any whistleblowing reports which have been made in the year. The last report was made to the RCC in May 2016 covering the period to March 2016.

Questions this paper addresses

- What whistleblowing reports have been made this year?
- What actions have been taken to investigate these reports?
- What issues do these reports raise?

Conclusion

1. Whistleblowing concerns can be raised in a number of ways: to line managers, other senior managers, through the Speak Up line, to the General Counsel via the email address whistleblowing@ GRO or in certain cases through external reporting lines such as to a regulator.
2. Postmasters can also raise concerns through the Grapevine reporting line and website, although concerns raised this way are investigated by the Security team.
3. In the period from end March 2016 to date only 2 whistleblowing reports have been received. This seems low compared to the number of reports received in previous years (3 in 2014-15, and 7 in 2015-16).
4. The reports in the current year related to the following:
    - A report was made to the FCA by an individual who was concerned that it appeared to be custom for staff at a specific branch to be able to initiate transactions under a single log-in. The FCA referred the concern to Bank of Ireland. Bank of Ireland requested Post Office's assistance to respond to the complaint. POL provided a response to BoI as to the required Horizon protocols and there has been no follow up from the FCA or BoI.
    - An anonymous report was made to the Speak Up line expressing concern as to the software procurement practices at Post Office. The CIO and Head of Procurement have been asked to review the software procurement processes and confirm that they are satisfied that the processes are appropriate so as to ensure that requirements are properly scoped and

POL00401624

relevant procurement processes followed. The advice received was that while anomalies will always occur, and the processes are cumbersome, they believe that overall the processes are sufficiently robust.

5. The whistleblowing policy is referenced in many of the other Post Office policies and the Code of Conduct. Since the beginning of the calendar year we have issued communications across the business reminding colleagues of the whistleblowing policy and advising how concerns can be reported. Interestingly the report raised in relation to software procurement followed one such communication.

Input Sought

The Committee is asked to note the report.

POL00401624

8.4) Identity Fraud Incident Report

Author: Rowan Hillery (Senior Manager – Customer Experience – Bank of Ireland UK Savings)

Meeting date: 4th May 2017

Executive Summary

Context

1. This paper updates the Committee on the recent Post Office Online Saver fraud case in the customer name of GRO

Questions this paper addresses

2. The paper outlines the details of the case and any resulting actions or proposals.

Conclusions

3. Bank of Ireland UK's (BoI UK) internal investigation concludes that the fraud occurred as a result of the customer's online login details being compromised. The exact method is unknown, though the investigation remains live in this regard.
4. The investigation has determined this is an isolated incident
5. BoI UK are reviewing the effectiveness of the existing control framework and operating model and will report on this in due course

Input Sought

6. The paper was requested by Post Office from BoI UK and is for discussion and noting at RCC.

POL00401624

The Report

1. **Case timeline**

Monday 3rd April:

- **21:23** - The first recorded instance of fraudulent activity occurs on the GRO PO Online Saver account. Both GRO nominated beneficiary accounts (a current account linked to the PO Savings account for the purpose of deposit and withdrawal) are deleted online and a new nominated beneficiary account is entered
- **21:33 -** The action of deleting and adding a new nominated beneficiary triggers the Servicing Platform to instigate a 1 working day freeze on the Online Saver account, preventing any transactional activity (e.g. withdrawals) for the period

Tuesday 4th April:

- **Overnight** - Account generates an automated letter ('nominated beneficiary letter') to the GRO home address advising of the change to nominated beneficiary account. To be sent in the day's post
- **21:14 -** A withdrawal is requested from the GRO Online Saver account of £6,500 to the new nominated beneficiary account (the NatWest sort code relates to a Hounslow branch). The withdrawal is completed the following day, Wednesday 5th

Thursday 6th April:

- **17:55** - the email address associated with the Online Saver is changed from GRO GRO to GRO GRO
- **17:56 -** a new Online Saver Issue 41 account is opened in GRO name, and GRO NatWest current account is linked to this new Savings Account
- **17:59** – a transfer of £1.00 from GRO existing Online Saver account is made to the new Online Saver Issue 41, completing the application process and triggering new account correspondence e.g. Welcome Letter

Saturday 8th April:

- **16:19** – GRO phones the Contact Centre and advises that he has received correspondence which leads him to believe a new PO Savings account has been opened fraudulently in his name
- During the call the agent correctly follows the process of raising a 'Hand off Task' to ensure Fraud are aware of the case on Monday. The agent speaks with their Team Leader and is additionally advised to place a 'block' on the account; the agent does not complete this action

POL00401624

- On this call, neither GRO or the agent make any reference to the balance on GRO genuine Online Saver Account
- **22:36 –** GRO emails Paula Vennells confirming they have lost £6,500:

  "Dear Paula,

  I don't know if you are still in post. We have experienced a fraud on a post office online account where a nominated account has been changed and £6500 extracted. We tried to phone your phone service for fraud today but told they do not work weekends and then tried to halt all access to this account. No passwords etc. have been compromised and we believe your operators have had changes made by mobile phone with insufficient security checks. We have reported this to the fraud crime division of the U.K. Police and have logged in this evening to see the account was blocked, which we find is not. Our names are GRO *Regards."*
- **23:07** - Paula replies to GRO apologising for the service and advising a senior manager will be in touch to deal directly. Copying to senior PO and BoI colleagues.

Monday 10th April:

- **09:09 –** GRO phones the Contact Centre again and is transferred to the Fraud team to discuss the circumstances of the case.

Wednesday 12th April:

- GRO emailed BoI to confirm safe receipt of the cheque fully reimbursing funds

2. **How was the Online Saver accessed?**

- All of the fraudulent activity was undertaken online via the PO Savings Servicing Site
- To access the GRO Online Saver account, 3 pieces of information are required:
  - User ID
  - Date of Birth
  - 6 Digit Security Number (6DSN)
- The GRO believed they were (both) victims of 'Sim Swapping'. This appears to be confirmed in the CIFAS records, where Tesco Mobile have registered an entry confirming as much – however, the GRO are stating that they never use their mobiles to login to their Savings accounts, nor do they store any logon information in their mobile phones
- 'Sim swap fraud' is typically used to describe a fraud where the fraudster rings the customer's network provider pretending to be the customer, cancelling an existing SIM and requesting the provider activates a new SIM card on a phone

POL00401624

in their control. This gives the fraudster control of the customer's mobile phone number

- This may, for example, be used to reset passwords in mobile banking apps, some of which require the customer to confirm a one off code that's texted to their mobile to verify the change in password
- While CIFAS records indicate the GRO were a victim of sim swapping, it appears unlikely that this was responsible for this case. The 6DSN was not changed on the account, and a request for a new one would have both invalidated the existing one and resulted in the new one being sent in the post. There is no way to reset online login details via mobile
- The GRO have since confirmed that the sim swapping occurred on the 6th April, which is after this fraud event.
- We do know the GRO were on a break in London at the time of the fraud (staying with family) and we also know that some of the fraudulent activity on their account was also conducted from IP Addresses located in London
- The GRO are keen to understand how this happened and have been open to working with us to resolve, for example they originally offered to allow us full access to their home computers if necessary to see whether they may in some way be compromised. We are unlikely to follow this course of action however as the fraudulent activity was from an ISP address in London.
- The GRO have confirmed that while they were away, no one had access to their home. In any case the evidence points to the fraudulent access taking place in London
- In conversation with our Complaint's Team the GRO advised that multiple (over 10) firms they have associations with (including other financial services firms) were fraudulently accessed. In particular they were unhappy with their mobile service provider who they claim gave access to the fraudster(s) despite apparently failing basic DPA questions

3. **Control environment**

Accessing the account:

- To access an account online 3 pieces of information are required:
  - User ID
  - Date of Birth
  - 6 Digit Security Number (6DSN)
- In this instance it's unclear how these details were compromised, this is the primary focus of the ongoing investigation

POL00401624

Applying a block to the account:

- When GRO first raised concerns on the call of Saturday 8th April, the Contact Centre Agent had the ability to place a 'block' on the account. This block would have prevented any further transactional activity on the account
- In this case the Contact Centre Agent correctly followed procedure and raised what is known as a 'hand off task', to alert the Fraud team to potential fraudulent account opening
- However, during the call the Agent placed GRO on hold while they sought advice from their Supervisor, who advised the Agent to also place a block on the account, as is the process in these instances. Upon returning to the call the Agent failed to place a block on the account. The Agent advised they forgot to do so after speaking further with GRO

Subsequent action:

- Following receipt of the GRO complaint we referred immediately to the Contact Centre for investigation. The calls were listened to and the Agent was immediately removed from live calls
- The Agent listened to the call and a fact find was conducted to identify any negligence or gaps in knowledge. It was established that the Agent was aware of the relevant fraud procedures but failed to implement them, and as a result of this HR gave the agent an official warning and the Agent was returned to live calls. Had the Agent been unaware of the procedures they would have undergone further training and live call quality assurance until such time that they were deemed competent
- It is important to note that had the Agent placed a block on the account, it may have provided some comfort to the GRO but the fraudulent withdrawal had already occurred at this stage, so it would not have prevented this
- All Agents within the Contact Centre were subsequently briefed to reiterate the correct process

5 working day freeze (changed to 1 working day freeze since 24th March):

- When the nominated bank account was changed on the account, a freeze was placed on the account for 1 full business day and a letter was triggered to the GRO address to advise of the change in details
- GRO nitial phone call was triggered by welcome correspondence from the new Online Saver Account
- If the freeze had remained at 5 days it is possible that in this instance the fraudulent transfer wouldn't have been completed before GRO first call, however it appears the opening of the new Online Saver account prompted the initial contact

POL00401624

4. **Next steps**

- BoI UK investigation leads us to believe this is an isolated incident of a customer login details being compromised – possibly via some kind of social engineering (responding to some kind of 'phishing', 'vishing', 'smishing') attack, or the customer enabling some form of remote access. Equally it may have involved someone within closer physical proximity, for example 'shoulder surfing' or direct device access
- The GRO recorded an 'incident' with the Police (Action Fraud) and were provided with an incident number. When our Fraud team contacted the Police they were advised that as this has not been 'crimed' it isn't under formal Police investigation. The GRO were under the impression it was, so we have spoken to them to advise they would need to raise this formally as a 'crime' to instigate a criminal investigation. We feel it is unlikely that the GRO will do this as there is less incentive given they have been recompensed.
- We are trying to establish how the GRO ogin details might have been compromised, though it may be that we never conclusively know, particularly if this case isn't recorded formally as a 'crime'
- Under normal circumstances return of funds may be held until investigations are at a more advanced stage, or a crime has been officially recorded. In this instance there may now be less incentive for the customer to pursue a criminal investigation as the refund has been received
- As part of the Service Site Redesign due later this year we are introducing email communications to customers where any personal details (including changes to nominated current account) are amended on their account. This will result in improved communication (where a valid email exists) to customers ensuring there is an opportunity for the customer to respond prior to the 1 working day freeze expiring
- A formal complaint was logged and the GRO have been kept appraised of the situation throughout our investigation via a senior complaint handler. While the GRO are apparently happy with the resolution of the case, we will be issuing the GRO a formal Final Decision Letter detailing the full outcome of our investigation once it has been completed.
- BOI are reviewing the Call Centre operating model which will include a review of opening hours.

Rowan Hillery

Senior Manager – Customer Experience – Bank of Ireland UK Savings

April 2017

POL00401624

Post Office Ltd
Risk & Compliance Committee meeting
4 May 2017

Location:

Boardroom 1.19 Wakefield , Finsbury Dials, 20 Finsbury Street, London, EC2Y 9AQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
MacLeod, Jane	
Alwen, Lyons	
Cameron, Alisdair	
Houghton, Rob	
Kevin, Gilliland	
Kirke, Martin	
Nick, Kennett	
Paula, Vennells	

Also in attendance

CoSec	

Additional access

Regan, Avene	