POL00110129

Risk and Compliance Committee Meeting
Monday 7 September 2015, 14:00 – 16:00
Boardroom 1.19 Wakefield, Finsbury Dials London

Dial in Details:
Freephone Number: GRO
Toll Number: GRO
Participant passcode: GRO #

Members:	Jane MacLeod (Chair) Alisdair Cameron Neil Hayward Alwen Lyons Nick Kennett Paula Vennells	**Attendees:**	Mike Morley-Fletcher Deana Herley Steve Miller Georgina Blair Adnan Killedar Charles Colquhoun David Hussey Kevin Gilliland
Apologies:	Garry Hooton		

	Agenda Item	Purpose	Timing	Paper	Owner
1	Risk profile update	Review updated profile	14:00 – 15:00 60 minutes	One A & B	Mike Morley-Fletcher
2	Risk incidents	Review recent incidents	15:00 – 15:10 5 minutes	Two	Steve Miller
3	Corporate Governance Code & Control Framework	Review update on approach to submission to ARC	15:10 – 15:15 5 minutes	Three	Mike Morley-Fletcher
4	Business continuity planning & management	Review interim incident management process & review proposal for BCM in POL	15:15 – 15:25 10 minutes	Four A, B & C	Steve Miller/Adnan Killedar
5	Corporate Insurance Programme renewal	Review plan prior to submission to ARC	15:25 – 15:35 10 minutes	Five	Charles Colquhoun
6	Litigation report	Review report prior to submission to ARC	15:35 – 15:45 10 minutes	Six	Chair
7	Internal Audit Report	Review latest update from Internal Audit prior to submission to ARC	15:45 – 15:55 10 minutes	Seven	Deana Herley
8	Committee minutes and actions	Agree minutes of last meeting and review actions	15:55 – 16:00 5 minutes	Eight	Chair

	Papers for Noting	Purpose		Paper	Owner
9	POMS RCC minutes	Note minutes of POMS RCC	-	Nine	Nick Kennett
10	Updated Cyber Security Charter	Noting	-	Ten	Julie George

POL00110129

RCC 7 SEPTEMBER 2015 PAPER ONE A

To: Risk and Compliance Committee 02/09/15

From Head of Risk and Assurance and Head of Risk MMF/ SM

GROUP RISKS - HALF YEAR RISK REVIEW

Purpose

1. The purpose of this session is to enable the Risk and Compliance Committee (RCC), at the half year, to review the Group Risk Profile and report to the ARC. In particular, to consider whether, in light of external or internal changes and experiences of rolling out the Three Year Plan, there have been any:

A) changes to our Group Risks

have the previous Group Risks changed in description, have new risks emerged, similar risks consolidated or current risks become less significant?

B) changes to the current evaluation of our Group Risks

have the current (net) evaluations of any Group Risks changed?

C) changes to the target evaluations for our Group Risks

in light of the above, but also considering our draft Risk Appetite Statement (which proposes the extent of risk we are willing to take), have our target evaluations for these Group Risks changed?

Preparation

2. **In advance of the session**, could you consider if there have been any changes you would like to suggest to the 27 Group Risk identified in May 2015 (see slide 1a of the support materials).

3. To suggest additional risks, we have worked with your Risk Champions to identify other potential risks from your Risk Registers – a "bottom-up perspective" and also added further options from a standard risk model (see slide 2).

4. To help expose gaps and overlaps, we have presented all these risks in a "Risk Universe" format, divided between external/ strategic, transformation, operational, financial and compliance risks (slides 1b and 2).

5. Please start with focusing on risks to **your own Business Area or Function**, before considering Group Risks "owned" by other RCC members.

Work steps

6. During the session we will discuss and agree your collective view on the most significant risks to the Group.

7. Once we have a revised list of Group Risks, we will re-confirm each risk's current evaluation using a Risk Profile/ Heat Map (see slide 3), taking into consideration any changes since May 2015.

8. And finally, we will trial, **for a few selected risks**, how we can use our draft Risk Appetite Statement (see slide 4) to help us identify target evaluations for each Red Risk – what we feel is the acceptable level of risk taking for each risk. This will show us the extent of Key Further Actions we will need to bring these risks

POL00110129

back to this target. The Risk team will continue this after the session with individual risk owners for discussion and approval at the next RCC.

Support materials

9. As background we include in the attached slide pack:

For part A) Changes to our Group Risks

Slide 1) a) our previous Group Risk Profile (May 2015), plus 1b) the risks displayed in a "Risk Universe" format to stimulate thoughts on completeness and help us spot any gaps or where we can consolidate similar risks

Slide 2) potential additional risks proposed by your Risk Champions at a recent risk review workshop, plus other risks suggested from a model Risk Universe

For part B) Changes to our current evaluations of our Group Risks

Slide 3) 3a) an example Risk Profile/ "Heat Map" mocked up for our risks and 3b) our Risk Evaluation Measurement Criteria Bands

For part C) Changes to the target evaluations for our Group Risks

Slide 4) our (draft) Risk Appetite Statement shown as a spidergramme.

Outcome

10. The intended outcome of this Risk Review session is for the RCC to update the previous Group Risk Profile, for changes to risks, their current (net) evaluations and target evaluations. This will:

a) help us to systematically challenge our progress with the Three Year Plan (and protecting our reputation).

b) influence decisions on the nature, extent and timing of Key Further Actions, to be completed post RCC, to achieve the Three Year Plan (and protect our reputation).

c) provide feedback on the draft Risk Appetite Statement as we look to refine this further through practical application.

d) provide assurance to the ARC (and so the Board) that the RCC is actively monitoring and challenging the Group Risks, ensuring that they are within our (draft) Risk Appetite and that appropriate Key Further Actions are being taken.

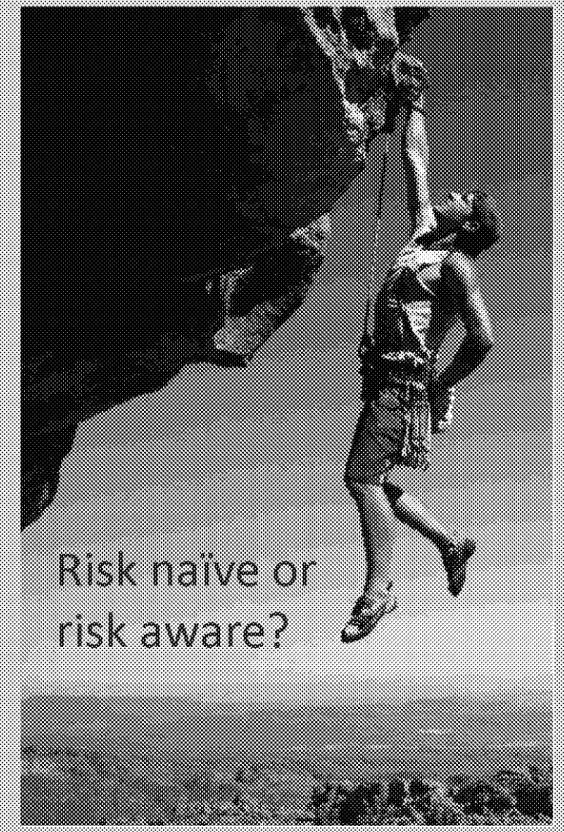
11. The output will be summarised in a Group Risk Profile (per slide 4) and Summary of Key Further Actions (per slide 5).

12. If you have any questions or comments beforehand, please feel free to contact the Head of Risk and Assurance, Mike Morley-Fletcher, or Steve Miller, Head of Risk.

POL00110129

Group Risks - Half Year Risk Review

Risk and Compliance Committee 7th Sept 2015



Mike Morley-Fletcher, Head of Risk and Assurance and
Steve Miller, Head of Risk

POL00110129

Contents

POL00110129

1a) PO Top 27 Risks – from May 2015's RCC

Category		Risk	I	L	Score
External	1	National Federation Sub Postmaster (NFSP) disrupts service (Neil Hayward)	4	2	8
External	2	Ineffective relations and agreement with Royal Mail (Martin George)	3	2	6
Strategic	3	Competitive threat (Martin George)	3	3	9
Strategic	4	BoI is not aligned (financially, strategically or contractually) to support POL (Nick Kennett)	4	2	8
Strategic	5	Loss of market share in mails due to inability to respond quickly to market developments leading to loss of revenue (Martin George)	3	2	6
Transformation	6	Strategic Objectives misalignment (David Hussey)	4	3	12
Transformation	7	Business transformation doesn't deliver objectives (David Hussey)	4	3	12
Transformation	8	Transformation function not designed and operating effectively (David Hussey)	4	3	12
Transformation	9	Benefit realisation (including Success Criteria) (David Hussey)	4	3	12
Transformation	10	CWU/Unite don't buy in to organisational change (Neil Hayward)	4	3	12
Transformation	11	Shareholder Agreement (Misalignment between programme and shareholder objectives) (David Hussey)	3	3	9
Operational	12	Delivery of new Front Office application delayed (Kevin Gilliland)	4	4	16
Operational	13	Failure of infrastructure and application environments (Lesley Sewell)	4	3	12
Operational	14	Transition Legacy IT Landscape (Lesley Sewell)	3	4	12
Operational	15	Manage complexity of change (capability) (Neil Hayward)	4	3	12
Operational	16	Risk that sales capability fails to deliver on FS growth targets (Nick Kennett)	3	3	9
Operational	17	Risk of strike action (Neil Hayward)	3	3	9
Operational	18	Manage volume of change (capacity) (Neil Hayward)	3	3	9
Operational	19	People capability and capacity are inadequate to deliver the strategic plan (Neil Hayward)	4	2	8
Operational	20	Proposition to agents/retailer becomes unattractive (leading to unsustainable network) (Kevin Gilliland)	3	2	6
Operational	21	Delivering customer experience and propositions that customers want (Martin George)	3	2	6
Financial	22	Government funding is insufficient to enable POL to operate until 2018 (Al Cameron)	4	3	12
Financial	23	Poor quality financial data and inadequate evaluation processes results in sub-optimal investment decisions (Al Cameron)	3	3	9
Legal	24	Unintentional breach of contractual terms (Jane MacLeod)	4	3	12
Legal	25	Non-compliance with law and regulation (Jane MacLeod)	3	3	9
Legal	26	Inadequate controls around the management of information result in a breach of company data (Jane MacLeod)	4	2	8
Legal	27	FS mis-selling risk: non-compliant product distribution, design or marketing or tougher regulation (Nick Kennett)	3	2	6

POL00110129

1b) PO Top 27 Risks – converted into Risk Universe format

To help us spot gaps and overlaps

PO RISK UNIVERSE part 1 v13.0 NOV

External/ Strategy *= external threat, wrong decision*	Transformation *= poor transformation*	Operational *= poor implementation*	Financial *= costs more*	Legal & Regulatory *= fail to comply*
5) Market developments vs Mail	**6)** BT misaligned with Strategic objectives	**20)** Network proposition unattractive to agents/ retailers/ become non-viable	**22)** Insufficient Government funding till 2018	**24)** Contractual breach
3) Competition vs Mail	**7)** BT doesn't deliver objectives	**21)** Fail to deliver customer proposition/ experience	**23)** Suboptimal investment decisions (e.g. due to poor MI)	**25)** Regulatory compliance failure (e.g. Competition, AML, ABC)
2) Royal Mail relationship/ agreement ineffective	**9)** BT benefits not realised	**12)** New Front Office application delayed		**26)** Data breach
1) NFSP disrupt service	**8)** BT function doesn't perform (design, operation	**16)** FS Sales capability fails to deliver		**27)** FS mis-selling
4) BOI not aligned to/ capable of supporting POL	**11)** BT objectives misaligned with Shareholder Agreement	**13)** Infrastructure/ applications fail		* Risks highlighted in red = Red Risk (score of 12 and above)
	15) Fail to manage complexity of change for staff (esp. ...)	**14)** Transition legacy IT landscape		Others are Amber Risks
	18) Fail to manage volume of change for staff (esp. FS Centre, Call Centre, Back Office)	**19)** People capability & capacity		
	10) CWU/ Unions vs BT change/ strike	**17)** Union strike action (Crown TP, pay, other)		

POL00110129

2) Suggestions for Additional PO Top Risks

To help us spot additional risks

PO RISK UNIVERSE part 2 v12dec10				
External/ Strategy	**Transformation**	**Operational**	**Financial**	**Legal & Regulatory**
N1) Lack of Government support for strategy (e.g. 25-40% cost savings reduce services) **N2)** Lack of Digital competency **N3)** Threat to PO Brand Reputation with Government, public, customers		**N4)** Viability of Mobile telephony trial offer **N5)** NTP lacks resource **N6)** Management of 3rd party suppliers/ Supply Chain service quality (IT, G4S, depots) **N7)** Call Centre transfer (Capita to HGS) **N8)** IT Security breach	**N9)** Unexpected cost (e.g. loss of RMG Warehousing contract, or Fujitsu exploiting exit costs)	**N10)** Contractual management process
Ex1) Market developments vs other (e.g. Government services, telecoms, FS, Retail Proposition) **Ex2)** Competition vs other (e.g. Government services, telecoms, FS, Retail Proposition) **Ex3)** Inadequate governance **Ex4)** Communication of Strategic objectives and plan		**Ex5)** Procurement **Ex6)** Health & Safety **Ex7)** Business continuity/ incident management failure **Ex8)** Fraud	**Ex9)** Liquidity **Ex10)** Bank covenants **Ex11)** Hedging **Ex12)** Pension deficit **Ex13)** Property impairment **Ex14)** Insurance protection **Ex15)** Financial Reporting and Control failure	**Ex16)** Litigation **Ex17)** Intellectual Property management

POST OFFICE

POL00110129

3a) Group Risk Profile/ "Heat Map" – an illustrative example

Post Office - Group Risk Profile - Top 11 Red Risks, plus 16 Amber Risks

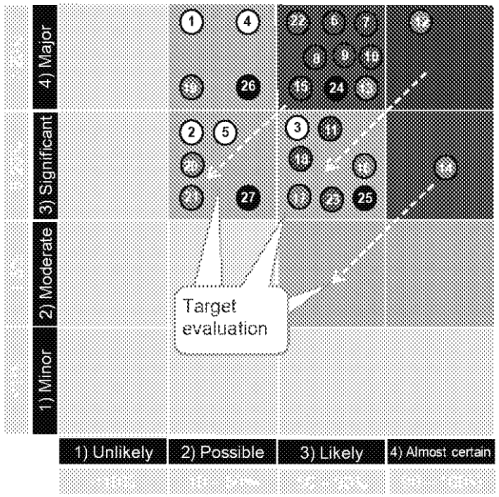
These are our Red Risks after review by the RCC (May 2015)

TOP *11* RED RISKS

illustrative

Description	Owner	Risk type	Change since last review	Net (P/I)	Target (P/I)
12) New Front Office application delayed	Kevin G	Ops	? - ?	4 – 4	? – ?
22) Insufficient Government funding till 2018	Al C	Fin		4 – 4	? – ?
6) BT misaligned with Strategic objectives	David H	Ops	? - ?	4 – 3	? – ?
7) BT doesn't deliver objectives	David H	Ops		4 – 3	? – ?
8) BT function doesn't perform (design, operation)	David H	Ops	? - ?	4 – 3	? – ?
9) BT benefits not realised	David H	Ops		4 – 3	? – ?
10) CWU/ Unions vs BT change / strike	Neil H	Ops		4 – 3	? – ?
15) Fail to manage complexity of change for staff (esp. FS Centre, Call Centre, Back Office)	Neil H	Ops	? - ?	4 – 3	? – ?
24) Contractual breach	Jane McL	Comp	? - ?	4 – 3	? – ?
13) Infrastructure/ applications fail	Lesley S	Ops		4 – 3	? – ?
14) Transition legacy IT landscape	Lesley S	Ops	? - ?	4 – 3	? – ?

RISK PROFILE (Net)



To help us visualise our key risks

POL00110129

3b) Measurement Criteria Bands – for evaluating risks

Impact Table

Weighting	Rating	Financial	Reputational	IT & Operations	Strategic	Regulatory	External Events
1	Minor	Potential financial loss of up to £1m.	Challenge worth noting but not of high enough impact to be of concern	Service disruption of up to one day Local (single site) disruption of up to 10 days	Slight delays in strategic programmes and/or slight reduction in expected benefits	Minor "technical" compliance issues identified	Local operational issues raised with member of parliament and/or letters to the editor of local press
2	Moderate	Potential financial loss of £1m - £5m.	Serious problem that would get attention of senior management but not be apparent externally	Local (single site) disruption of more than 10 days Regional service disruption of up to 5 days	Delays in strategic programmes/delays in launching products which result in loss of expected benefits and negative impact on return on investment. Target operating model will not deliver all of the expected benefits	Breach of compliance issues, but very limited / no scope for customer detriment, non-reportable to regulators	Concerns or complaints raised by public groups or industry associations to local government and press coverage
3	Significant	Potential financial loss of more than £5m and up to £20m.	Causes concern to shareholders broader public	Regional service disruption of more than 5 days National service disruption at major locations of up to 5 days	Major delays in programmes, resulting in loss of revenue and non-realisation of benefits. Target operating model loses relevance due to changed operating environment and customer requirements	One or more material or significant regulatory / compliance issues, customer detriment identified and reportable to regulators	Concerns or complaints raised by public groups or industry associations to government bodies with potential to create government policy adjustment with respect to POL and media coverage
4	Major	Potential financial loss of over £20 million.	Catastrophic to the long-term survival of the business	National service disruption at major locations or critical business function for more than 5 days	Failure of programmes to meet requirements/deliver expected benefits and/or change programme delivers an operating model which is not relevant	One or more major regulatory compliance issues with clear customer detriment issues which could lead to regulatory censure and could adversely affect POL's ability to conduct business	Government enquiry into operational inadequacies or financial loss with a more certainty that government will alter policy with respect to POL strategy

Likelihood Table

Weighting	Rating	Description
1	Unlikely	Less than 10% chance the risk will become reality within the foreseeable future
2	Possible	More than 10% chance but less than 50% chance the risk will become reality
3	Likely	More than 50% but less that 90% chance the risk will become reality
4	Almost certain	More than 90% chance that the risk will become reality within the next 3 years

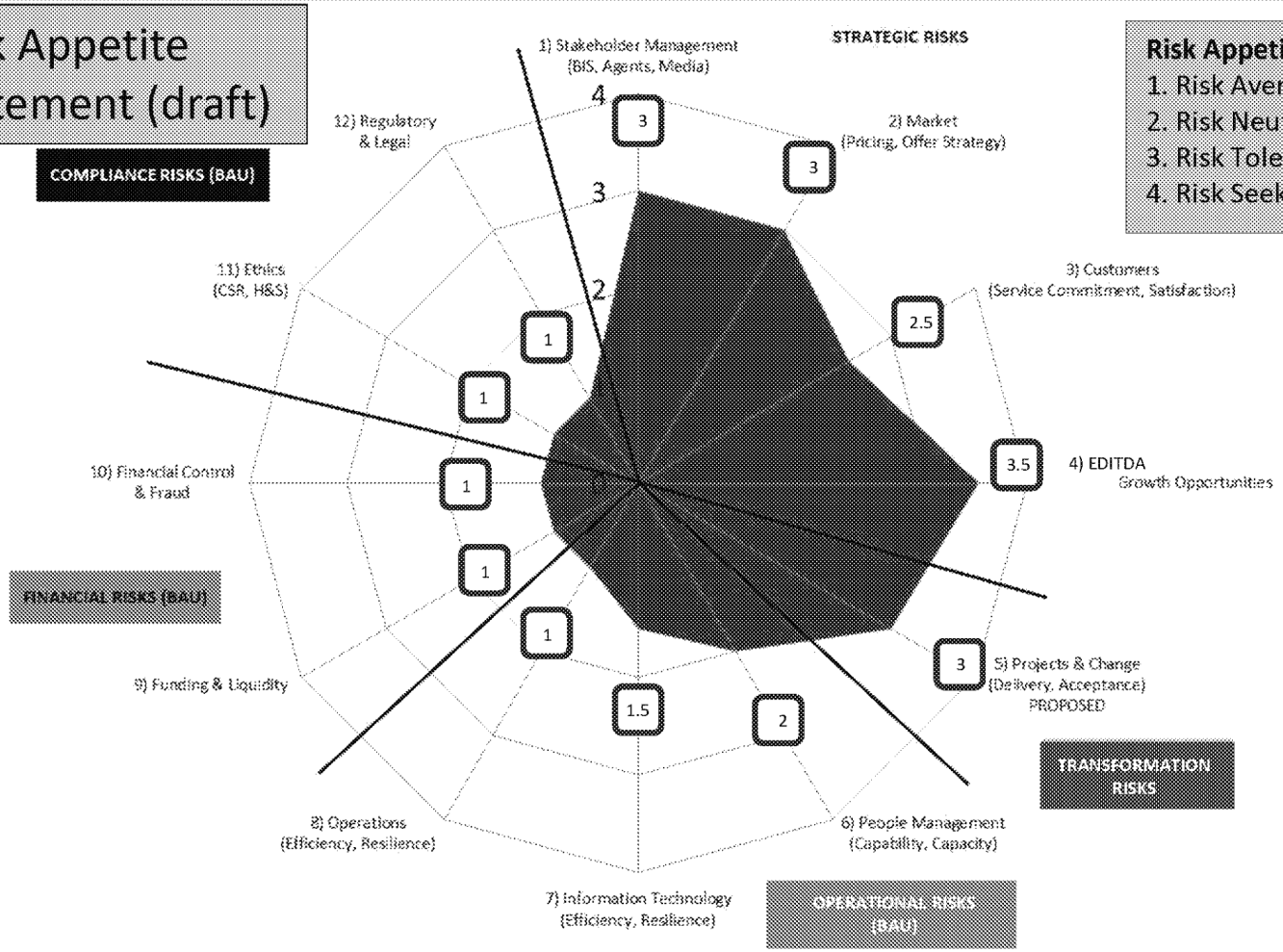
POST OFFICE

POL00110129

4) Risk Appetite – for assessing target evaluations

Risk Appetite Statement (draft)

To help us set target evaluations



Risk Appetite scale
1. Risk Averse
2. Risk Neutral
3. Risk Tolerant
4. Risk Seeking

POL00110129

5) Summary of Key Further Actions - an illustrative example

RED KEY RISKS						KEY FURTHER ACTIONS	
Ref) Title: description	Owner	Risk Cat	Change since last review	Net (I/L)	Target (I/L)	Details **Red**: 2 or more actions are overdue **Amber**: 1 action is overdue **Green**: All actions are on track	Status of Actions
12) New Front Office application delayed	Kevin G	Oper	↑ ? - ?	4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline) • Key Further Action 3 (owner, timeline) • Key Further Action 4 (owner, timeline)	
22) Insufficient Government funding till 2018	Al C	Fin		4 – 3	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline) • Key Further Action 3 (owner, timeline)	
6) BT misaligned with Strategic objectives	David H	Transf	↑ ? - ?	4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
7) BT doesn't deliver objectives	David H	Transf		4 – 3	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
8) BT function doesn't perform (design, operation)	David H	Transf	↑ ? - ?	4 – 3	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
9) BT benefits not realised	David H	Transf		4 – 2	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
10) CWU/ Unions vs BT change / strike	Neil H	Transf		4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
15) Fail to manage complexity of change for staff (esp. FS Centre, Call Centre, Back Office)	Neil H	Transf	↓ ? - ?	4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	
24) Contractual breach	Jane McL	Comp	↑ ? - ?	4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline) • Key Further Action 3 (owner, timeline)	
13) Infrastructure/ applications fail	Lesley S	Oper		4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline) • Key Further Action 3 (owner, timeline)	
14) Transition legacy IT landscape	Lesley S	Oper	↓ ? - ?	4 – 4	? – ?	• Key Further Action 1 (owner, timeline) • Key Further Action 2 (owner, timeline)	

To help us check progress on Key Further Actions

POST OFFICE

POL00110129

RCC 7 SEPTEMBER 2015 PAPER TWO

INCIDENTS FOR RCC on 7 September 2015

Incidents: Detail of the incidents reported to risk in the past two months (caveat: this does not purport to be a full incident population)

	Title	Risk Universe	Event	Cause	Impact	Actions	Owner
1.	**Multiple Transtrack failures**	Operational	• Unable to scan cash & stock into Transtrack • System unavailability	• Failure to import data from POLSAP & back up failed • DNS & connectivity issues	• Work around required manual inputting into Transtrack causing operational delays • Billing of external customers delayed	• CSC manually imported import files & restarted back ups • Reconfiguration of desktops to restore connectivity	Russell Hancock
2.	**Travel Money online service failure**	Operational	• Lack of connectivity to core Travel Money Card services on POL website	• First Rate internal firewall issue	• Customers unable to place Travel Money Orders Online or top up Travel Money Cards	• First Rate resolved issues across their internal firewall which restored service	IT
3.	**POL website down**	Operational	Website unavailable on: • 8th August – 4 minutes • 17th August – 4 minutes • 18th August – 5 minutes • 22nd August – 4 hrs 25 min • 23rd August – 8 hrs 57 min • 27th August – 35 min • 29th August – 15 hr 45 min	• Likely to be due to distributed denial of service attack (DDoS)	• Customers unable to use website • Problems with Drop & Go customers in branches with some accounts being locked and mail being stranded in branches	• Skyscape (cloud service provider) worked with supplier to validate security settings. • Extensive monitoring put in place to detect such attacks in the future	
4.	**POL SAP unavailability**	Operational	• Multiple instances of users unable to access POL SAP via webportal	• Known issue with E-portal	• Both Cash Centres and the Finance Service Centre unable to process cash transactions.	• POL SAP issue resolved by CSC. E-portal issue under continued investigation.	
5.	**Core Finance System unavailability**	Operational	• Users saw blank screen on logging on	• ERP server was offline	• 100+ users unable to use system	• Server restarted by CGI	
6.	**Breach of Welsh Language**	Operational	• FOIA request highlighted that Welsh branches not	• Failure to pick up requirement when	• Risk of challenge (Judicial Review) to all re-locations of	• Welsh translations of adverts for vacant	John B Jenkinson

POL00110129

Incidents: Detail of the incidents reported to risk in the past two months (caveat: this does not purport to be a full incident population)

	Title	Risk Universe	Event	Cause	Impact	Actions	Owner
	Scheme		advertised in Welsh as well as English on business opportunity website. • This is a breach of a commitment made in POL's own Welsh Language Scheme	website designed	branches in Wales	branches being prepared.	
7.	**Lift safety certificates not in place**	Legal & Regulatory	• Interim Property Compliance Manager identified that no current independent lift safety certificates in place for circa 60 lifts	• Insufficient contract management of facilities management hard services provider (Norland)	• Risk of Health and Safety prosecution. Risk of significant fines and jail sentences.	• POL Property is working with Norland to obtain independent safety certificates.	Kevin Seller
8.	**CO_2 poisoning**	Legal & Regulatory	• Incident of CO_2 poisoning due to faulty boiler in Chesterfield	• Inadequate handover from RM and ROMEC to POL and Norland	• Health and Safety Executive involved	• Written confirmation requested from Norland that all necessary steps have been taken	Kevin Seller
9.	**Swindon Warehousing Agreement**	Financial	• RM threatening to stock providing stock to Swindon unless budget codes are allocated • RM threatening to terminate & re-tender warehousing agreement • Potential overbilling claim of £10	• Absence of express terms in MDA or Swindon Warehousing Agreement dealing with distribution costs to network	• Potential of no stock being distributed to branches, leading to operational disruption and impact on revenue • Termination of warehousing agreement	• Legal advice provided to Mails team	Gordon Rose

POL00110129

RCC 7 SEPTEMBER 2015 PAPER THREE

To: RCC

From: Steve Miller

Date: 28 August 2015

Re: Update on Policy and Control Framework, and compliance with UK Corporate Code

Required:

1. For information. Committee members to be aware of the approach to these two key framework items which will be presented to Audit and Risk Committee

Background:

2. Papers on two framework and governance elements will be presented to Audit and Risk Committee in September. This note summarises the approach; the two elements are closely linked.

3. Policy Framework:

a. POL needs a common approach to managing a top-down suite of policies. A proposal is in preparation outlining the process and timetable for establishing scope, process and timetable.

b. The proposal will set out the key steps; specify requirements, develop the design, test and evaluate, report and feedback, then prioritise and implement.

c. Effective policy framework and governance is vital to understanding how we manage the key risks. Policies will include definitions of exposures, how these are controlled and managed, responsibilities and accountabilities. A set of measures for each significant risk and control assists putting risk appetite limits into operation in the line.

d. This will start with the Corporate Services related policies to use as a test, and will be followed by a prioritisation exercise to identify the business critical elements to work on first.

4. Approach to compliance with UK Corporate Code (The Code):

a. The costs of compliance with the risk management requirements of The Code are high, both centrally and across business areas. Given the current state of risk management maturity, compliance will need significant investment.

b. However, the risk management section of The Code can be used as an internal benchmark for our performance. Industry is currently showing a range of practices; we need to ensure that our response is the most appropriate, showing cost-benefit in managing the risk profile, and in oversight of the internal control framework.

c. Consequently, meeting Code requirements has dependency on the effective implementation of the Policy Framework.

d. A paper will be presented to Audit and Risk Committee updating the gap analysis on the Annual Assessment process which was produced in March. FRC guidance includes a series of questions boards are advised to use in conducting the assessment. These questions have been used to assess the POL risk framework status in line with current industry practice and summarised key actions for the next six months.

Steve Miller

28 August 2015

POL00110129

RCC 7 SEPTEMBER 2015 PAPER THREE

POL00110129

RCC 7 SEPTEMBER 2015 PAPER FOUR A

To: RCC

From: Steve Miller

Re: POL – Business Continuity update plan and Interim Incident Management Procedure

Background:

1. The RCC in its last meeting in August 2015 reviewed the Business Continuity Planning status and action plan and requested a more detailed paper covering the resource requirements.
2. Whilst business continuity including wider incident management is an area currently undergoing review, following the evacuation of Finsbury Dials out of hours on Wednesday 26 August 2015, a potential gap was identified in the current incident management procedure.
3. It was felt appropriate to implement an interim procedure.

Issues:

4. The Risk Team has prepared a Business Continuity resource plan covering both the business resources (1st line) and the Central Business Continuity team (2nd line).
5. The plan is spread over three phases with varying resource requirements which is a mixture of:
    a. Contract staff (in Central Risk Team – 2nd Line) totalling 2.35 FTE across all phases.
    b. POL operational business units to provide SME / line management resource (1st line). This has been totalled and given a sum FTE value across POL of 3.5 FTE commitment across all phases
6. The current incident management procedure is focussed on IT and does not effectively cover non-IT incidents.
7. This was highlighted on 26 August 2015 when Finsbury Dials had to be evacuated and the building security was not aware of who to contact in the Post Office and how to coordinate related activities.
8. This was brought to the attention of the CoSec and CEO who requested an urgent review and an interim Incident Management plan has been developed and distributed across all Post Office administration buildings.

Actions:

9. RCC are asked to consider the resource plan and approach and:
    a. Approve the recruitment of an interim Senior BCM to deliver Phase 1 and commence Phase 2 on initial six month contract. Senior BCM to be supported by an additional contract BCM after three months (subsequent to Phase 1 completion).
    b. Support the time commitment required from the 1st line business areas running business critical processes in engaging with this initiative and providing appropriate SME.
    c. Review and approve the approach in the attached paper **(Paper 4B)**.
10. The Property and Risk Teams have developed an interim procedure on the request of the CEO and Company Secretary which is being presented to the RCC for their comments and feedback **(Paper 4C)**.

Steve Miller

2 September 2015

POL00110129

BUSINESS CONTINUITY

POL Business Continuity Planning

Specification for development

Steve Miller
26 August 2015

POL00110129

Background

It was appreciated by RCC that the resource for BC management is low. This paper details actions required for adequate BC management, and estimates time and cost.

The resource assessments are based on:

- Central Risk Team engaging contract resource for Phase 1 and 2.
- Business units engaging with the risk team at each phase and providing SME resource.

Phase 1 would be completed as rapidly as possible by a contract Senior Business Continuity Manager in 3 months.

This provides an assessment of the most urgent actions, and starting points for governance, risk assessment and incident management. A further resource of Business Continuity Manager would be added at the end of Phase 1 to begin executing the action plan.

Completion of Phase 2 would be expected to give a reasonable BC management response for POL, but at low level of maturity.

Phase 3 delivers increased maturity, and sets up BCP as a BAU activity with programmes of assessment, testing and review. The five most critical areas identified in Phase 1 will have BC plans by 30 June 2016.

POL00110129

Action Required

ACTION:

RCC are asked to consider this approach and:

- Approve the recruitment of a interim Senior BCM to deliver Phase 1 and commence Phase 2 on initial six month contract. Senior BCM to be supported by an additional contract BCM after three months (subsequent to Phase 1 completion).
- Support the time commitment required from the 1st line business areas running business critical processes in engaging with this initiative and providing appropriate SME.
- Review and approve the approach below.

POL00110129

Resource Requirement

Summary of resources:

Resource is a mixture of requirements on existing operational staff (1st Line) and contractors (2nd Line). The table below totals the demand on business units (1st Line) across POL into a single FTE number.

In summary, 1st Line is 3.5 FTE and 2nd Line is 2.35 FTE.

	Resource	Phase 1	Phase 2	Phase 3
First Line	Business units will need to engage with Central Risk Team to: • Assist with data for initial review • Prepare BIAs and recovery plans • Test and annual review	**.5 FTE** Line to send all existing BC material; • BIAs • Recovery plans • Test regimes • Incident management	**1 FTE** Line to engage with: • Identifying business critical activities. • Testing incident management • Developing BIA • Developing recovery plans	**2 FTE** Line to: • Incorporate BCM into BAU activities • Engage with annual review and testing • Review BIA and recovery plans
Second Line	Contract resource for Phase 1 and 2: Phase 3: Decision point for permanent / contract	**.35 FTE** • Review of current status • Developing policy and approach.	**1 FTE** • Develop BIA method • Implement CMT / incident management • Map business critical activities • Roll out BIA & recovery planning	**1 FTE** • Build BCM into BAU • Deliver suite of BC plans • Run testing programme and review

POL00110129

Summary

Phase	Deliverables	Cost (£k)	Time (days)
1	• Review existing activities and collect all existing BC plans • Provide high level gap analysis • Establish BCM structure for crisis / incident management and develop process • Develop overarching policy statement and POL strategic approach to BCM	**£121k**	**1st line: 129** **2nd line: 93**
2	• Test CMT and incident management processes • Develop risk assessment and business impact analysis methodology and set resilience levels • Identify and map business critical activities and plan programme of BIA assessments	**£243k**	**1st line: 255** **2nd line: 225**
3	• Build BCM into a business as usual activity and begin first iteration • Delivery of complete suite of BC plans, plus testing programme	**£337k**	**1st line: 445** **2nd line: 255**
	TOTAL	**£701k**	**1st line: 829** **2nd line: 573**

The above summarises the deliverables for each phase and cost estimate.

Cost estimates are based on the assumption that there will be 20 BC plans required for POL based on the number of business units, key locations and functional areas. Allocation of 1st line (business process owner) resource requirements is based on the number of days per plan/business unit with a cost £400 per day (although this is opportunity cost).

Second line (Central Risk Team) resource has calculated at one senior contractor starting in October 2015 at £750 per day and a second contractor joining from January 2016 month four at a cost of £500 per day.

POL00110129

Summary

Phase	Cost (£k)	Deliverables	Oct - Dec 15	Jan – Mar 16	Apr – Jun 16	Jul – Sep 16	Oct – Dec 16	Jan – Mar 17
1	£121k	Review of BC plans	x					
		High level gap analysis and prioritisation of areas	x					
		BC policy and strategy	x	x				
		BC management structure	x	x				
2	£243k	CMT and incident process		x				
		Risk assessment and BIA methodology		x	x			
		Map of business critical activities		x				
		Plan for BIA assessments		x				
3	£337k	Integrate BCM in BAU activities			x	x		
		Delivery of BC plans (based on agreed prioritisation)			x	x	x	x
		Testing programme for BC plans			x	x	x	x

POL00110129

Phase 1: BCP Triage I

Triage	Deliverable / actions	Resource	Cost (£k)
Policy statement	Review and finalise/update existing BC policy. Identify critical services (suppliers and customers) and define levels of disruption. Communicate to stakeholders (GE, RCC, ARC, SLT, CMT and key area managers)	1st line: 4 days	1.6
		2nd line: 6 days	4.5
Crisis management	Review processes for crisis management, including different teams, forums. Review the different incident management processes Draft a consolidated approach to incident management for POL, including response by incident severity, invocation of different management teams Communicate incident management plan (timetable appropriate testing as a minimum).	1st line: 16 days	6.4
		2nd line: 8 days	6.0
Current planning and responses	Canvas key members of SLT (supply chain, security, ISAG, IT) for existing BIA and BCP Conduct high level review of adequacy and effectiveness (when planned, when tested etc).	1st line: 17 days	6.8
		2nd line: 36 days	27.0
Structures	Establish structures and groups (CMT, Business Protection, BC Steering Group – if still required) Identify first line BCP owners for business critical areas and define responsibilities. Define ToR and responsibilities for groups and individuals Desktop walkthrough of incident management structures Provide training, education and information	1st line: 77 days	30.8
		2nd line: 35 days	26.25

POL00110129

Phase 1: BCP Triage II

Triage	Deliverable / actions	Resource	Cost (£k)
Gap analysis	Prepare a gap analysis from the above and review Phase 2 in light of finding. Prepare options for proceeding (appetite, policy statement, methodology, plan shape, testing requirements – and frequency, recovery requirements)	1st line: 10 days	4.0
		2nd line: 3 days	2.25
Review point	Present analysis to RCC and GE for review. Determine how to progress and resources allocated (i.e. continue contract, permanent BCM, run as project)	1st line: 5 days	2.0
		2nd line: 5 days	3.75
	TOTAL PHASE 1	1st line: 129 days	51.6
	(nb: Total contractor cost for Phase 1 = £69.75k)	**2nd line: 93 days**	**69.75**
		TOTAL	£121k

NB: The target for delivery of Phase 1 is six months. This is based on the dependency of timely engagement from business owners and SLT members and access to any existing documentation.

POL00110129

Phase 2: Governance I

Framework and Governance	Deliverable / actions	Resource	Cost (£K)
Training	Hold training for CMT and selected SLT members on BC Management, POL requirements and implementation.	1st line: 35 days	14.0
		2nd line: 5 days	3.125
Crisis management plan	Hold initial CMT meeting and exercise Communicate and test incident definitions and levels	1st line: 10 days	4.0
		2nd line: 10 days	6.25
Incident management procedure	Communicate incident management procedure across wider POL community Provide training and education Publication (net, gatefolds, call cascades).	1st line: 15 days	6.0
		2nd line: 20 days	12.5
Assessment method	Define and agree BIA methodology Identify most significant areas to assess	1st line: 20 days	8.0
		2nd line: 30 days	18.75
Response and recovery	Define recovery levels and resilience (and cost)	1st line: 40 days	16.0
		2nd line: 40 days	25.0

POL00110129

Phase 2: Risks and Recovery I

Risk Profile	Deliverable / actions	Resource	Cost (£K)
Map existing plans	Engage with most critical areas from Triage phase and identify any existing BC plans Review for; testing, adequacy (within policy statement)	1st line: 20 days	8.0
		2nd line: 25 days	15.625
Map prioritising business critical systems	Using high level process map/systems landscape (see slide appendices) to identify business critical processes in line with policy statement and appetite..	1st line: 50 days	20.0
Map business critical processes	Identify business critical systems.		
Map business critical suppliers / outsource providers	Identify business critical suppliers Identify process / system / supplier dependencies.		
Map criticality of property / locations	Map any upstream / downstream processing dependencies across suppliers and processes. Identify any hotspots in activities Develop 'overlay' to extract the business critical systems, processes, suppliers and property / locations on to a delivery map and use to understand critical junctures of services and suppliers.	2nd line: 30 days	18.75

POL00110129

Phase 2: Risks and Recovery I

Risk Profile	Deliverable / actions	Resource	Cost (£k)
Roll out plan (Phase 3)	Plan programme of business impact analysis, continuity and recovery planning for critical business areas based on analysis, resource allocation and budget in first line.	1st line: 60 days	24.0
	This is the largest piece of work, has the most moving parts and will require the most analysis. It will also require commitment from the business / first line resources.	2nd line: 60 days	37.5
Review point	Present analysis to RCC and GE for review. Determine how to progress Phase and review resource requirements/allocation (i.e. continue contract, permanent BCM)	1st line: 5 days	2.0
		2nd line: 5 days	3.125
	TOTAL PHASE 2	1st line: 255 days	102.0
	(nb: Total contractor cost Phase 2 = 140.625 Phase 1 + Phase 2 = £210.375)	**2nd line: 225 days**	**140.625**
		TOTAL	£243k

POL00110129

Phase 3: Governance II

Framework and Governance	Deliverable / actions	Resource	Cost (£K)
Monitoring / reporting	BCMS strategic management Up to date BC policy	1st line: 25 Days	10.0
	Current / up to date BC appetite, processes and objectives. BCMS implementation/integration	2nd line: 15 Days	9.375
Enhancements	Maintain and improve BCMS	1st line: 25 Days	10.0
	Reviewed plans based on business change/technology change/test results/actual event	2nd line: 10 Days	6.25
Assurance	Threat and risk assessment faced by the PO.	1st line: 25 Days	10.0
	Action plan for improvements of BCMS. Confirmation of roles and responsibilities.	2nd line: 15 Days	9.375

POL00110129

Phase 3: Risks and Recovery II

Risk Profile	Deliverable / actions	Resource	Cost (£k)
Impact analysis	BIAs across the PO business units/functions based on agreed prioritisation. BIAs reviewed and "owned" by process/system owners.	1st line: 60 days	24.0
		2nd line: 60 days	37.5
Development of plans	Process / systems based BC plans documented by the 1st line under BCM guidance. Identification of training requirements Training of staff.	1st line: 200 days	80.0
		2nd line: 45 days	28.125
Testing	Develop testing programme CMT exercise, incident management processes, call cascades	1st line: 70 days	28.0
	Test business unit BC plans. Level of testing to be dependent on criticality of process and complexity of supporting systems.	2nd line: 90 days	56.25
Review / update of plans	Review / update plans based on test results, changes in business, changes in technology or people.	1st line: 40 days	16.0
		2nd line: 20 days	12.5
	TOTAL PHASE 3	**1st line: 445 days**	178.0
	(nb: By Phase 3 all costs should be in BAU (approx 1 FTE based on current understanding) and this represents rough cost pa @ same rate)	**2nd line: 255 days**	159.375
		TOTAL	**£337k**

POL00110129

Appendices

The following have been included for information purposes:

1. High Level Operating Model: Demonstrates extent of current operating model – 'as is' from the Transformation Design Authority pack.
2. Process Model: Top level processes identified by McKinsey in their TOM design work in 2014.
3. Technology Model: Post Office current systems landscape
4. Property Model: Principal office and supply chain locations

POL00110129

High Level Operating Model

POST OFFICE®

AS-IS Capability Model v0.9, 09/07/15

Strategy & Planning

Face to Face

Agency Stores
Training
Enquiry
Sale/Application
Transact
Service Customer
ATM
SSK
Mailwork

Crown Stores
Enquiry
Sale/Application
Transact
Service Customer
ATM
SSK
Training

Notes
Coins
Foreign
Non Secure Stock
Secure Stock

Retail Delivery

Telephone & Mail
Supply Chain External CS
Bank Of Ireland
Fidelity Information Svcs
Family Investments
BoI Personal Finance
BISL Limited
Aviva Life & Pension
Collinson Insurance Svcs
JP Morgan Europe
Fujitsu
VOW
CCU
POEX
Customer Complaints (CCU)

Digital
PO Web
Enquiry
Sale/Application
Transact
Service Customer
Supplier
Supplier
POEX

IT
Managed Services
IT Service
IT Account Management
Technology Office
IT Transformation & IT Change
Finance

Network Business Support (NBSC)
Branch Support
Agent Recruitment & Remuneration
Security & Fraud Analysis
Branch Audit

Network Support
Network Design & Analysis
Crown Planning & Performance
Income Support
Operational Training
Operational Support
Facilities & Property
Finance

Supply Chain
Finance
Training

Executive Complaints

Mails
Account Management
Product Management
Proposition Development
Business Development
Supplier Management
Finance

Retail
Account Management
Product Management
Proposition Development
Business Development
Supplier Management
Finance

Govt. Services
Account Management
Product Management
Proposition Development
Business Development
Supplier Management
Finance

Telephony
Account Management
Product Management
Proposition Development
Business Development
Supplier Management
Finance

Financial Services
Insurance
Travel Money
Savings & Investment
Mortgages & Transactions
Banking & Payments
Finance

Commercial Development

Brand & Marketing
Customer Analysis
Brand Analysis
Marketing & Comms
Customer Experience
Marketing Planning
Digital Web Mgmt

Finance
Planning, Budgeting & Forecasting
Taxation
Project Accounting
Profitability Analysis
Treasury

People & Engagement
People Strategy
Channels
Agent Remuneration
Agent Relations
Internal Comms
IR & Employee Relations
Public Affairs
Pensions
Rewards
Learning, Resourcing, Talent & Performance
PR
Policy & Briefing
Employee & Agent Engagement
Planning & Events

Corporate Services
Legal
Security & Fraud
Internal Audit
Risk & Compliance
Finance

Property Operations

FSC
Client Settlement & Account Payable
Customer Driven Enquiries
Accounts & Reporting
Debt Recovery & Account receivable
Open Item Enquiries
Change

HRSC
Agent Recruitment
Employee Payroll
Employee recruitment
Agent Remuneration
Learning & Development Admin
Employee Support

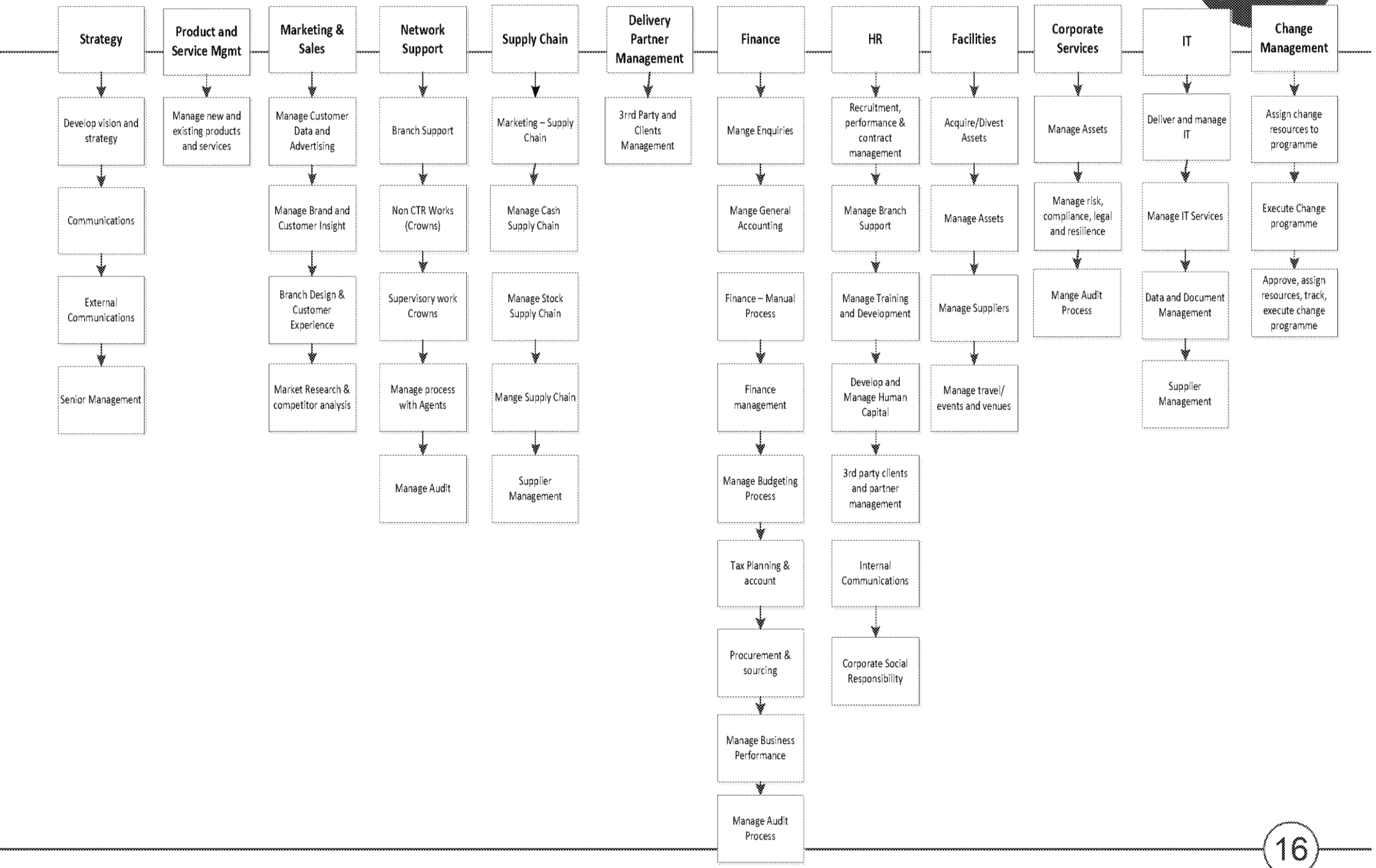
Risk, Banking Reg & Strategy
Training & Competence

Transformation Management
Financial Control
Design
Transformation Delivery
Business Readiness
Risk Management
Communications

Key
Network and Sales
CFO
Commercial
Financial Services

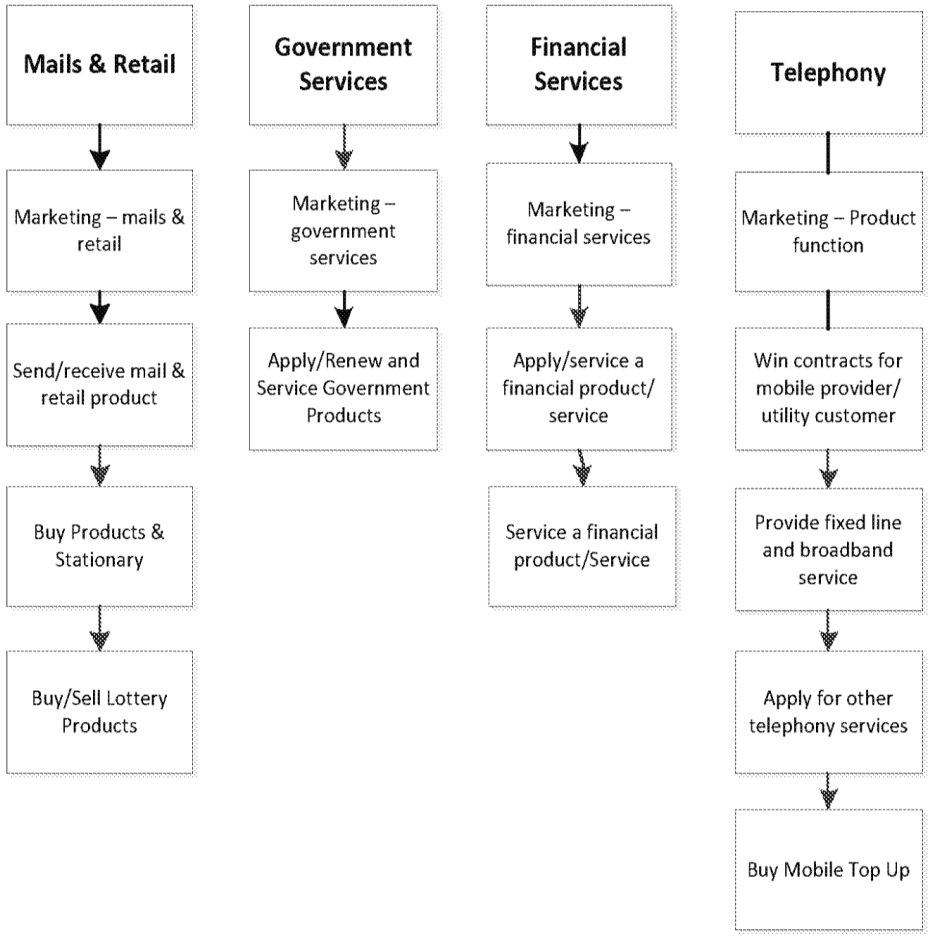
POL00110129

Process Model



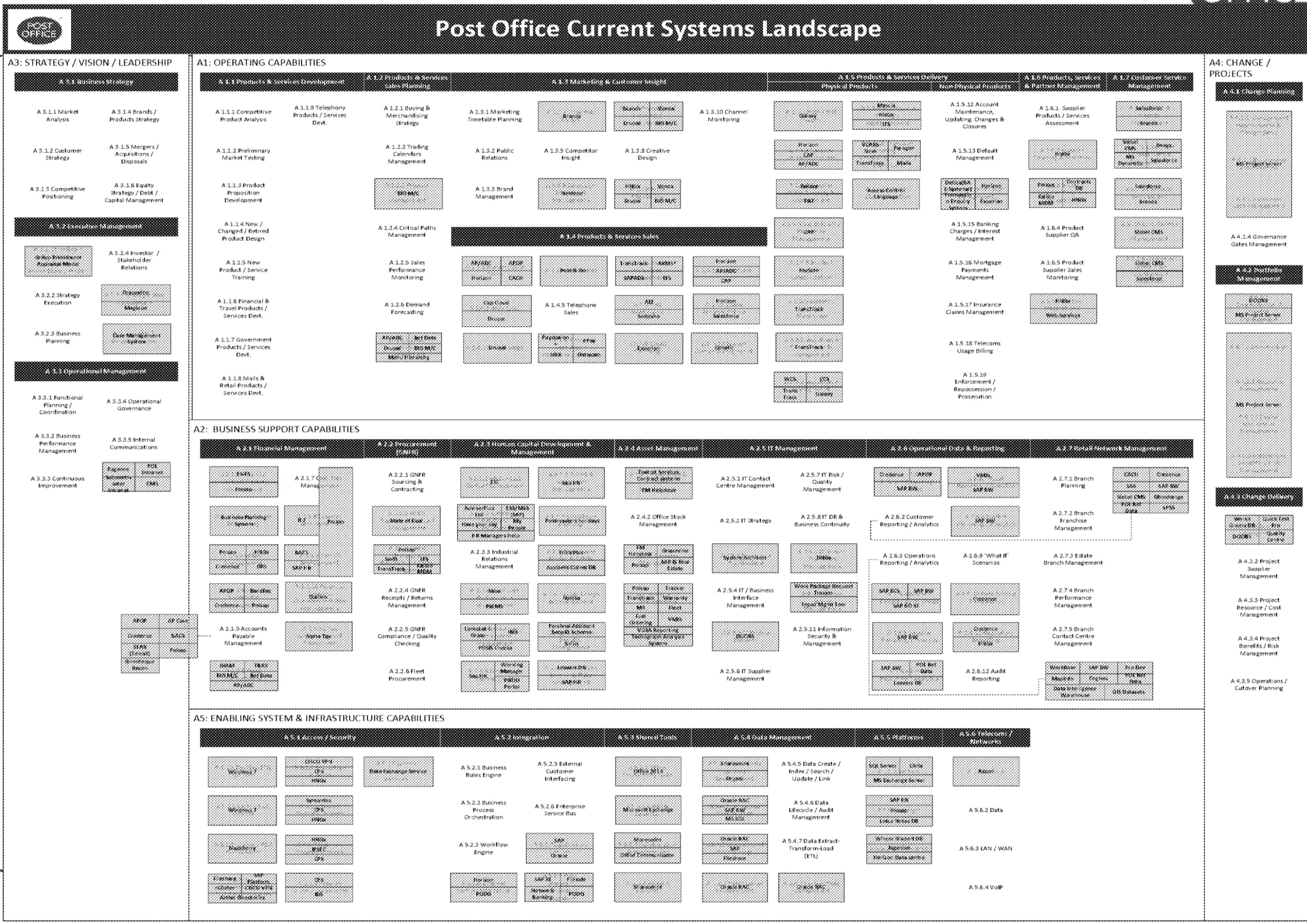
POL00110129

Process Model



POL00110129

Technology Model



POL00110129

Property Model

Principal Office Based Functions Locations

Supply Chain Locations

POL00110129

Interim Incident Management Procedure

Author:	Andrew Masson - Post Office Ltd	**Date:** 27 August 2015
Authorised:	Mark Lawrence – Post Office Ltd Adnan Killedar – Post Office Ltd	**Date:** 28 August 2015
Issued: 28/08/15	Version 1	**Review:** 01/10/15

POL00110129

Interim Incident Management Procedure

Scope

This procedure only applies to the premises identified below:-

(**Please Note:** Network Offices, Supply Chain - Paper & Metal Store facilities and Information Technology Incidents are excluded as there are separate arrangements in place for these):

Bark Street	Finsbury Dials
Bristol	St Helens
Chesterfield	Swindon
Dearne	Wealdstone

Role of Single Point of Contact

1). You have been identified as the Single Point of Contact (SPoC) for your building (see attached Appendix 3.

2) The SPoC should access the "Stay Calm Guide" for information regarding the Building Contact Details (blank example see attached). Each site should have a completed copy which should be periodically reviewed. The SPoC is responsible to ensure that the Building Contact Details are up to date and reviewed every three months or after any major changes. The SPoC should hold a copy of the "Stay Calm Guide" that can be accessed if they are not at the premises and also share this with their nominated deputy when they are covering. The SPoC should immediately contact the NBSC (08:00 to 18:00 Monday to Saturday GRO or Grapevine (24 hours) GRO depending on timing of the incident, and following initial contact with any required emergency services if required.

Building Contact Details.pdf

4). As primary contact for your site you may receive notification of an incident. If so you are required to conduct a **severity assessment**, and then take the **appropriate resultant action**. If you are out of contact, then your voice mail must contain the details for your empowered deputy who must be fully aware of this process and appropriate contacts, and be ready to act.

POL00110129

Severity Assessment

5) In the event of an incident the SPoC should assess the severity (see below) and invoke a proportionate response:-

- **Minor Incident** – Little internal impact with no external customer impact and minimal staff impact, resolution timescales measured in hours (for example localised flood within a premise due to burst pipe).

- **Moderate Incident** – Additional internal impact but no customer impact. May require short term alternate facilities for staff, resolution timescale extended to several days (for example a localised flood effecting fixed wiring or damaging computer equipment, or a fire causing predominately smoke / decorative damage).

- **Significant Incident** – Any incident where there is a potential external customer impact, or where staff are required to work remotely or from a different premises (for example substantial flooding, fire damage, extended loss of utilities or incident external to Post Office premises restricting access).

- **Major Incident** – Confirmed impact to external customers, extensive destruction / impairment of Post Office premises preventing access or use for an extended period (for example serious fire within the building, structural damage due to weather, terrorist activity or similar).

Resultant Action

6) The SPoC should contact any emergency services, if required.

7) The SPoC should then contact the NBSC (08:00 to 18:00 Monday to Saturday) GRO or Grapevine (24 hours) GRO depending on timing of the incident. The details of the incident, any actions taken and any support required should be advised.

8) Following this, the SPoC should act per below, depending on the severity assessment:

Minor Incident Response:

- Contact appropriate contractors/SN@P Property Helpdesk Tel GRO to progress remedial works, details should be on the 'building contact details' document so it is important that this is reviewed on a regular basis e.g. every 3 months and updated as appropriate. Agree with Communications Team; GRO and Managers for any affected areas to advise staff as to the progress and resolution timescales. Issue a general communication to the Group Executive, Executive Team and colleagues.

POL00110129

Moderate Incident Response:

- Manage resolution with required contractors; escalate for support from IT and Property colleagues as required (contact points listed in Appendix 4). Work with Communications Team and Managers for affected areas to advise staff as to the progress and resolution timescales. Issue a general communication to the Group Executive, Executive Team and colleagues.

Significant Incident Response

- The SPoC should invoke a conference call with the Business Protection Team (see Appendix 1), initial contact should be via email and text message identifying a Conference Call Number and time of call with a brief description of the incident and location. The SPoC will set up the call which will then be chaired by the appropriate lead. Next steps will be agreed with owners identified for actions which should include communications and engaging relevant contractors. The schedule and location of additional meetings and calls should be agreed at this initial conference call.

Major Incident Response:

- The SPoC should invoke a conference call with the Major Incident Emergency Group (see Appendix 2), initial contact should be via email and text message identifying a Conference Call Number and time of call with brief description of the incident and location. The SPoC will set up the call which will then be chaired by the appropriate lead. Next steps will be agreed with owners identified for actions which should include communications and engaging relevant contractors. The schedule and location of additional meetings and calls should be agreed at this initial conference call. A debrief and lessons learnt exercise is required for all major incidents and the Post Office Business Continuity Manager can provide assistance in carrying these out.

POL00110129

Appendix One

Business Protection Team				
First Name	**Last Name**	**Designation**	**Contact Number**	**Email Address**
Adnan	Killedar	Business Continuity Manager	GRO	GRO
Steve	Beddoe	Sr Ops Manager-Service Delivery		
Joe	Connor	Head of HR Services		
Jeff	Smyth	TBD		
Roger	Gale	General Manager-Crown Sales		
Andy	Garner	Head of Managed Service		
Julie	George	Head of ISAG		
Jonathan	Hill	Head of Risk-FS		
Rod	Ismay	Head of FSC		
Michael	Larkin	Head of Sales Capability		
Kevin	Lenihan	Project Principal-IS		
Mark	Ellis	Supply Chain Director		
Alana	Renner	Head of Engagement		
John M	Scott	Head of Security		
Richard Z	Walden	Internal Communications		
Kevin	Seller	Head of Govt Innovations Programme		

Appendix Two

Major Incident Executive Group				
First Name	**Last Name**	**Designation**	**Contact Number**	**Email Address**
Jane	MacLeod	General Counsel	GRO	GRO
Kevin	Gilliland	Network Director		
Alwen	Lyons	Company Secretary		
Alisdair	Cameron	Chief Financial Officer		
Tom	Wechsler	Chief of Staff		
Lesley	Sewell	Chief Information Officer		
Mark R	Davies	Communications Director		
Martin	George	Commercial Director		
Neil	Hayward	HR Director		
Nicholas	Kennett	Financial Services Director		
Paula	Vennells	Chief Executive		
David	Hussey	Business Transformation Director		

POL00110129

Appendix Three

Post Office Properties - SPoC Contacts								
	Primary Contact				Secondary Contact			
Building	First Name	Last Name	Contact Number	Email Address	First Name	Last Name	Contact Number	Email Address
Finsbury Dials	Andrew	Masson	GRO	GRO	Mark	Lawrence	GRO	GRO
Chesterfield	Deborah	Holmes			Alison	Bolsover		
Bristol	Becky	Portch			Christine	Williams		
Swindon	Patricia	Powton			Jonathan	Duncan		
Bark Street	Jayne	Bradbury			Joe	Connor		
Dearne	John	Cawthorn			Dean	Whitehea		
St Helens	Lucy	Lewis			Joanne	Faulkner		
Wealdstone	Audra	Mirjah-Clark			Vinal	Chauhan		

POL00110129

Distribution

Document Distribution		
Major Incident Executive Group	**Business Protection Team**	**SPoC Contacts**
jane.macleod GRO	adnan.killedar GRO	andrew.j.masso GRO
kevin.gillilan GRO	steve.beddoe GRO	deborah.holme GRO
alwen.lyons GRO	joe.connor GRO	rebecca.l.portch GRO
alisdair.cameron GRO	Jeff.Smyth GRO	patricia.powtor GRO
tom.wechsle GRO	roger.gale GRO	jayne.bradbury GRO
lesley.j.sewel GRO	andy.garner GRO	john.cawthorn GRO
mark.r.davies GRO	julie.george GRO	Lucy.Lewis GRO
martin.george GRO	jonathan.e.hill GRO	audra.mirjah-clarke GRO
neil.hayward GRO	rod.ismay GRO	mark.d.lawrence GRO
nicholas.kennett GRO	michael.larkin GRO	alison.bolsover GRO
paula.vennells GRO	kevin.lenihan GRO	christine.williams GRO
david.hussey GRO	mark.ellis GRO	jonathan.r.duncan GRO
	alana.renner GRO	joe.connor GRO
	john.m.scott GRO	dean.whitehead GRO
	richard.z.walden GRO	joanne.faulkner GRO
	kevin.seller GRO	vinal.chauhan GRO

POL00110129

RCC 7 SEPTEMBER 2015 RESTRICTED PAPER FIVE

MEMORANDUM FOR: **The Board of Post Office Limited**

FROM: **Alisdair Cameron, Chief Financial Officer**

SUBJECT: **Corporate Insurance Programme 2015/16**

DATE: **22 September 2015**

Recommendation

1. It is recommended that the Board's approval for the renewal of this programme, noting the 14% reduction in premium in addition to the c30% reduction achieved since separation from RMG which is in addition to the c90% reduction in payments for claims during that period.

Executive Summary

2.1 This is the fourth anniversary of the PO stand-alone Insurance Programme following the split from the RMG insurance programme in September 2012.

2.2 PO confirmed its intent to appoint Lockton Companies LLP to act as its corporate Insurance Adviser with effect from 1 July 2015.

2.3 The insurance programme is due to be renewed on 1 October so negotiations are continuing which may further improve terms – no policy will be renewed on terms worse than those at Annex 3 unless of course there is a material change to Post Office's risk profile before renewal (eg a major claim).

2.4 As part of the insurance review POL will utilise the Official Journal of the European Union ("OJEU") process for the procurement of insurances where applicable.

2.5 PO and Lockton agreed all quotations received from Insurers will be subjected to the following scoring matrix to demonstrate best value to PO:

Criteria	Points	Weight
Price for Insurance cover	600	60%
Assessment of Policy Cover	250	25%
Claims Service	100	10%
Added Value and Innovation	5	5%

Key Insurance policies

2.6 The key corporate insurances currently in place are (more detail at Annex 3):

- Crime
- Directors and Officers Liability
- Property Damage/Increased Cost of Working
- Terrorism

POL00110129

- Employers Liability
- Public Liability
- Motor Fleet (Commercial and Private)
- Cyber Liability (specific Government Contracts only)
- Professional Indemnity (Government Contracts only)
- Personal Accident/Travel
- Special Contingency

Claims

2.7 This has been another good year for PO with regards to claims, with a relatively stable pattern of claims notified, which is better than envisaged when our standalone programme was set up.

2.8 It should be noted that PO now has clear claims procedures in place, with QBE handling all liability and motor claims. This has led to a substantial drop in amounts paid out in claims since RMG managed the process. Full details are attached in Annex 2.

Summary of Insurance Review

2.9 A review has been undertaken of all the major risks and relevant insurance policies. Full details are contained in Appendix 1, however in summary, the main findings of the review are:

Our insurances are fit for purpose

- Some policies will not be renewed (Contractors All Risks)
- Our deductibles are high for a company POL's size so these should be reduced where there is no impact on premium
- Leveraging our risk and claims data to reduce premium where possible
- We are obtaining quotations for Professional Indemnity Insurance across POL rather than split policies for POMS and POL as now.

2.10 Some of the savings are being achieved by having 2 year deals

POMS

2.11 A review will be undertaken over the next 12 months, when POMS is fully operational , to see if it is economic to manage some of this insurance programme through POMS.

Financial Metrics

3. The total premium for a year for all the insurance policies will be no greater than £1.267m (last year's equivalent £1.441m) exc Insurance Premium Tax of 6%.

Conclusion

4. It is recommended that the insurance programme should be renewed for a premium of no more than £1.267m (exc Insurance Premium Tax).

Alisdair Cameron
Chief Financial Officer

POL00110129

APPENDIX 1

POST OFFICE LTD - INSURANCE REVIEW - AUGUST 2015

POST OFFICE LTD - INSURANCE REVIEW - AUGUST 2015 Appendix 1

RISK (currently insured)	Insurer/ Premium	Covering	Deductible	Additional Comments/Recommendations	Recommendation
PROPERTY DAMAGE					
TERRORISM					
EMPLOYERS LIABILITY					
PUBLIC/PRODUCTS LIABILITY					
MOTOR FLEET					
CRIME					

IRRELEVANT

POL00110129

RISK (currently insured)	Insurer/ Premium	Covering	Deductible	Additional Comments/Recommendations	Recommendation
DIRECTORS AND OFFICERS LIABILITY					
PROFESSIONAL INDEMNITY - POL WIDE					
PROFESSIONAL INDEMNITY (GOV CONTRACTS)					
PERSONAL ACCIDENT/TRAVEL					
CYBER LIABILITY					

IRRELEVANT

POL00110129

APPENDIX 2

Claims recorded under the POL insurance programme are as follows. All other policies are claims free.

Motor Fleet – Claims Summary

UW Year	Claim Count	Total Paid	Open Reserves	Gross Incurred
2012	207	£232,281.77	£19,664.00	£251,945.77
2013	348	£244,168.97	£128,917.00	£373,085.97
2014	303	£79,247.31	£215,624.00	£294,871.31
Total	**858**	**£555,698.05**	**£364,205.00**	**£919,903.05**

Employers / Public Liability – Claims Summary

UW Year	Policy Class	Claim Count	Total Paid	Recoveries	Open Reserves	Gross Incurred	Net Incurred
2012	**Employers' Liability**	8	£25,482	£0	£36,707	£62,189	£62,189
	General Liability	17	£57,101	£0	£46,516	£103,617	£103,617
	Total	25	£82,584	£0	£83,223	£165,807	£165,807
2013	**Employers' Liability**	10	£22,727	£0	£98,665	£121,392	£121,392
	General Liability	20	£23,388	£0	£113,855	£137,243	£137,243
	Total	30	£46,115	£0	£212,520	£258,634	£258,634
2014	**Employers' Liability**	18	£3,666	£0	£155,051	£158,717	£158,717
	General Liability	5	£0	£0	£47,454	£47,454	£47,454
	Total	23	£3,666	£0	£202,505	£206,171	£206,171
Total	**Total**	**78**	**£132,364**	**£0**	**£498,247**	**£630,612**	**£630,612**

POL00110129

APPENDIX 3

Brief synopsis of Insurance cover

1. Crime Insurance

1.1 PO historically has one of the largest stand-alone Crime policies in the UK insurance market, insuring to a limit of GBP600 million, and is a requirement for membership of the Bank of England's Note Circulation Scheme. The policy covers all risk of crime including theft by employees. The policy carries a GBP1million excess and is insured by QBE and others. This is PO's largest external premium spend.

2. Property Damage/Increased Cost of Working/Terrorism.

2.1 PO has a Property Damage policy, insuring the full value of properties valued at above GBP1m. There is a GBP10 million increased cost of working limit. There have been no claims.

2.2 Zurich is the current insurer and there is a GBP1million excess on the policy. Terrorism is purchased separately.

2.3 We have obtained alternative quotations for the Property insurances from several Insurers, the most attractive at this stage of negotiations being QBE. We have alternatives from Mitsui and ACE and are in discussions with other insurers. We expect to see circa 10% premium savings on a like for like basis.

2.4 QBE Insurance currently underwrite a large proportion of Post Office Ltd's insurances. QBE are one of the world's top 20 general insurance and reinsurance companies, employing 17,000 people in 38 countries and with a strong London market presence. Their gross written premium in 2014 was US$16bn and they are currently S and P A+ rated (insurer financial strength rating)

During this year's remarketing exercise QBE have additionally quoted competitive terms on POL's Property Damage & Business Interruption insurance.

Lockton have an in house market security committee which monitor the suitability and security of all Insurers that they place business with. QBE Insurance is currently an approved insurer by the committee.

3. Combined Liability Insurance (Employers/Public Liability)

3.1 PO has a combined Liability programme from QBE, providing GBP50m of coverage on both Employers Liability and Public Liability. This carries a GBP250k excess per loss with an annual aggregate cap of GBP2.35m (incl motor below). QBE handle the claims below the excess and is reimbursed by PO on a quarterly basis. This is a relationship that works well.

POL00110129

4. Motor Fleet Insurance

4.1 PO has two motor fleets (Commercial vehicles and Private Cars) both insured via QBE.

4.2 The policy is placed in the same way as the Combined liability (namely, with a GBP250k excess with claims below the excess paid by QBE and reimbursed by PO on a quarterly basis).

5. Directors and Officers Liability

5.1 This policy provides cover for PO directors and officers where they are sued as a result of a wrongful act, resulting from something that they are alleged to have done while acting as a manager of PO.

5.2 In addition, the policy will respond if there is an investigation into an act that they are alleged to have committed.

5.3 The policy currently has a limit of GBP60m. An insurance review last year looked at whether reducing this limit to GBP40m (saving approx. GBP20,000 in premium) was viable. As a large organisation, it is felt that the current limit of GBP60m is the minimum level that PO should have and therefore should be retained.

6. Professional Indemnity

6.1 This policy was purchased to meet the Government Service Contracts contractual requirements. The policy has a GBP10m limit and covers a breach of professional duty by PO resulting in a third party loss. The policy covers Civil liability, defence costs and expenses, libel and slander (committed by PO or any person employed by PO). The policy has a GBP250k excess. QBE are the lead insurer.

6.2 Our strategy, particularly in relation to our FI products, and the increased risks this brings to the organisation, means that we should consider purchasing Professional Indemnity insurance for the whole organisation. The review is underway and insurers have spent some time with PO assessing the exposures. POL's cover will be extended to align with POMS so this decision will be taken to allow renewal of both policies on Dec 1st.

7. Cyber Liability

7.1 This insurance is purchased as a specific requirement for the DVLA and Border Agency contracts and is a broad cover, extending to breach of privacy, extortion, network security, as well as breach of data. This policy renews in April 2016.

7.2 One of our key strategic risks relates to data protection and data integrity. The Insurance review has identified that consideration should be given to purchasing Cyber Liability across PO which would offer us a level of protection in the event of a significant loss.

POL00110129

APPENDIX 4

POST OFFICE LTD – INSURANCE REVIEW – AUGUST 2015 – PREMIUM TABLE

Class of Insurance	2014 Expiring Premium	Estimated 2015 Premium
Property Damage & Business Interruption (Inc. Contractors All Risks)	£ 84,134	£ 75,000 (TBC)
Terrorism	£ 24,600	£ 17,000 (TBC)
Combined Employers Liability & Public/Products Liability	£ 225,000	£ 180,000
Motor Fleet	£ 362,862	£ 308,751
Crime	£ 675,500	£ 625,000 (TBC)
Directors & Officers Liability	£ 65,000	£ 58,500 (TBC)
Professional Indemnity – POL	*£ 105,000*	*Will extend for 2 months until December 2015*
Professional Indemnity – POMS	*£ 49,500*	*Renews December 2015*
Personal Accident / Travel	£ 3,500	£ 3,573
Cyber Liability	*£ 85,800*	*Renews April 2016*
Total	**£ 1,440,596***	**£1,267,824***

*Total excludes policy not due/being renewed on 1st October 2015:

- Cyber
- Professional Indemnity – POL
- Professional Indemnity – POMS

These are assumed to continue at the existing premium in the above comparison. Combined Employers Liability & Public/Products liability and Motor's quotes are based on 2 year deals.

All premiums exclude Insurance Premium Tax currently at 6%.

POL00110129

RCC 7 SEPTEMBER 2015 PAPER SIX

To: RCC

From: Rodric Williams

Date: 28 August 2015

Re: Litigation Half Year Update

Purpose:

1. Risk and Compliance Committee to review the following Litigation report for the 2015/16 Half Year Briefing Book, prior to submission to ARC.

POL00110129

RCC 7 SEPTEMBER 2015 PAPER SIX

Litigation Report Extract for 2015/16 Half Year Briefing Book:

17. Litigation and Claims - Potential Claims regarding Horizon (Half Year 2015-2016)

Background

17.1 Post Office Limited has received various claims from postmasters (PMs) alleging defects in the Horizon system and Post Office's internal processes. These allegations were initially made more than 3 years ago in 5 claims brought through solicitors Shoosmiths. Similar allegations have been made by the "Justice for Subpostmasters Alliance" (JFSA) and advanced through PMs' MPs.

17.2 Following discussions with James Arbuthnot MP and JFSA, in July 2012 independent investigator Second Sight Support Services Ltd (Second Sight) was appointed to carry out a review into these allegations.

17.3 On 8 July 2013, Second Sight published a Report finding shortcomings in Post Office's internal training and support to PMs on the Horizon system, but no systemic problems with Horizon itself.

17.4 Following Second Sight's July 2013 Report, on 27 August 2013 Post Office launched an Investigation and Mediation Scheme aimed at understanding and resolving individual complaints made about Horizon.

Mediation Scheme

17.5 The Scheme received 150 applications, 136 of which were investigated in detail (the remainder being either ineligible or swiftly resolved) and progressed through the Scheme under the direction of a Working Group chaired by retired Court of Appeal Judge Sir Anthony Hooper, and comprising representatives from Post Office, Second Sight, and JFSA.

17.6 On 10 March 2015, Post Office agreed to mediate all cases remaining in the Scheme except those the subject of a previous court ruling, and closed the Working Group.

17.7 On 9 April 2015 Second Sight produced a "Briefing Report - Part Two", ostensibly to assist applicants understand certain themes common to multiple applications. Although the report found that the majority of the investigated branch losses were caused by "*errors made at the counter*", Post Office was unable to endorse Second Sight's report as a whole, and produced a Reply to correct inaccuracies and provide information excluded by Second Sight.

17.8 Second Sight has now completed its reviews of the individual Scheme cases and its engagement with Post Office has ended. Steps have been taken to ensure the preservation and return to Post Office of all documentation considered or generated as part of its engagement.

17.9 Currently, 59 cases are waiting for mediation to be scheduled or take place. All mediations will continue to be overseen by the Centre for Effective Dispute Resolution (CEDR), the independent organisation appointed by Post Office to administer the mediations.

17.10 Orchestrated by the JFSA, 43 applicants indicated their wish to withdraw from, or postpone, mediation until such time as the Scheme is 'reviewed by Parliament'. We have however written to all Applicants with cases approved for mediation requesting that they contact CEDR by 4 September 2015 to arrange a date for mediation, failing which we would consider their case closed.

Political Activity

17.11 The Scheme and allegations concerning Horizon continue to generate Parliamentary activity following the Westminster Hall Debate on 17 December 2014 and a BIS Select Committee hearing on 3 February 2015.

17.12 Andrew Bridgen MP, now leading the Parliamentary campaign following James Arbuthnot's retirement, asked for a judicial enquiry during an Adjournment debate on 29 June 2015 and during Prime Minister's Questions on 1 July 2015.

17.13 The position being communicated by BIS is that no inquiry is necessary as those with complaints have existing routes to resolution available to them (mediation, appeal or litigation). It is however possible that a newly constituted BIS Select Committee could bring

POL00110129

further scrutiny in due course. Post Office's Communications team is managing this activity with support from the Mediation Scheme team.

Legal Activity

17.14 To date, no claim has been made against Post Office in the civil courts, and no appeal has been made to the Court of Appeal against any conviction obtained in the criminal courts, arising out of the matters raised in Second Sight's reports or through the Scheme.

17.15 "Horizon" has been raised as a defence to one court claim brought by Post Office for repayment of a £50k branch debt. Post Office Legal and external solicitors are managing this case, which is in the early stages of the court's case management procedure,

Media Activity

17.16 The Scheme and allegations concerning Horizon continue to generate media interest, most significantly the BBC Panorama programme "Trouble at the Post Office" broadcast on 17 August 2015.

17.17 We are continuing to engage with the BBC about the programme, which we consider broadcast untrue and damaging allegations about Post Office. The programme did not however produce anything with which we were unfamiliar, and so far has not been picked up widely by other media.

17.18 Post Office's Communications team continues to manage this media activity.

Regulatory Activity

17.19 Post Office is engaging with the Criminal Cases Review Commission (CCRC) in relation to 20 applications made by former PMs seeking a review of their convictions, 16 of whom are applicants to the Scheme. The CCRC can refer a case to the Court of Appeal if its review identifies new evidence or legal argument which gives rise to a "real possibility" that the conviction would be overturned on appeal.

17.20 Post Office's Legal team is liaising with the CCRC so as to comply with its statutory obligations under the Criminal Appeals Act 1995, and has provided to the CCRC very substantial documentation for review. The CCRC has not indicated how long it will take to complete its reviews, but it is it not anticipated that they will be completed before calendar year end 2015.

17.21 Post Office also received 45 simultaneous "Data Subject Access Requests" (DSARs), 42 of which have been made by Scheme applicants. Post Office's Mediation Scheme, Legal and Information Security teams are coordinating Post Office's responses to the DSARs in accordance with the Data Protection Act 1998.

17.22 Post Office has applied substantial resources to the DSARs, and anticipates completing its responses by the end of October 2015. Applicants may however make formal complaints to the Information Commissioner's Office if they are not satisfied by the timing or content of the response they receive.

POL00110129

Internal Audit
Risk and Compliance Committee Report
September 2015

POL00110129

Post Office Internal Audit RCC Report – September 2015

1. Audits completed since last RCC.

Audit	Key Findings	Status (01/09)
Contract Management	• Supplier contract portfolio is not fully known. • Contract Management Framework (CMF) remains in draft (since its development in 2012) and requires further development, finalisation and implementation. • Staff have the ability to define their own roles and responsibilities. • Management are unable to effectively foresee and manage expiration of contracts. • Analysis and management of risks to drive contract management.	• Final Report issued (see Appendix 1). Actions will be followed up with management as appropriate.
Financial Crime	• Staff are not clear on where and how to report suspicions or concerns. • Effective mechanisms to prevent and detect fraud and corruption are not incorporated into policies, procedures and systems. • Focus of proactive / reactive activity is directed towards customers and customer facing areas of the business. • There is no corporate / PO wide approach.	• Report discussed with relevant management and actions agreed.

POL00110129

Post Office Internal Audit RCC Report – September 2015

2. Work in progress.

Audit	Key Findings	Status (01/09)
FS Conduct Risk	• Subject to management clearance – detail on findings will be shared with members once agreed.	• Draft report completed. • Preparation for clearance in progress – Mgt clearance w/c 14 September (due to leave).
Drop and Go Review - Enhancement	• Number of Drop and Go active accounts are unknown. • Transaction data is not personalised. • No communication solution has been developed covering : **When will the Online Mails portal go live? What can I tell my customers? What is happening with Click and Drop?** • Postmasters and central fund make up the difference when some customers have insufficient funds in the Drop and Go account. There is no formal process for debt recovery.	• Fieldwork complete. • Findings with management, report in draft.
Drop and Go Review - Product Development	• Negative behaviour scenarios were not considered during testing. • Insufficient regression testing performed resulting in bugs going un-detected at migration. • Project risks were not transparently communicated to stakeholders. • Project management principles were not formally applied. • Scale of change and interdependencies were not understood. • Scope and deliverables changed a number of times yet the business case was not rebaselined.	• Fieldwork complete. • Findings with management, report in draft.

POST OFFICE

POL00110129

Post Office Internal Audit RCC Report – September 2015

2. Work in progress cont.

Audit	Key Findings	Status (01/09)
IT Towers Delivery On-going Assurance	• Fieldwork on-going. • Majority of emerging issues raised have been addressed by the recent restructure and creation of new Post Office Programme Manager roles.	• First highlight report agreed and shared with management.
Management Information	• Meetings held with the Finance Directors to determine sample of critical metrics for testing. • Fieldwork commenced.	• Fieldwork in progress. • Reporting due end September.
Fujitsu exit	• Fieldwork was placed on hold pending Board decision (and internal restructure) – updating approach with management	• Current position being determined with management prior to recommencing audit. • Co source resource being secured to commence this work in September
Telecoms	• Terms of Reference agreed. • Fieldwork commenced.	• Fieldwork in progress. • Reporting due end September.

POL00110129

Post Office Internal Audit RCC Report – September 2015

3. What we will do - Next 3 months.

Audit	Sponsor	Comments	Fieldwork Timing	Completion
Assurance Framework	Jane MacLeod	• Assessment and review of the assurance providers within PO. • Terms of Reference drafted and shared with Risk team. • Linked to Business Transformation programme.	On-going	TBC
Data Protection	Jane MacLeod	• Assessment and review of ISAG Data Protection processes and controls in place.	November	November
Fujitsu exit	Lesley Sewell	• Controls and mechanisms in place to control Fujitsu services and minimise exit cost. • Initial work commenced but subsequently held pending Board decision – updating approach with management.	September	October

POL00110129

Post Office Internal Audit RCC Report – September 2015

4. Other matters.

Area	Comments
Business Transformation	Independent Transformation Assurance (ITA) reviews have started. A Front Office Mobilisation review and Portfolio Governance, Management and Change Methodology Design review are currently underway supported by Internal Audit, due to report in September 2015. Deloitte has been appointed as the assurance partner to deliver the on-going ITA plan. They will be on-boarded in early September before starting to deliver reviews later in the month .
Mails Collection Service	This has been incorporated into the Drop and Go findings and associated actions which is currently with management for their responses.

POL00110129

Post Office Internal Audit RCC Report – September 2015

4. Other matters cont.

Area	Comments
Property Regulatory Compliance	Internal audit has continued to work with Legal in assisting Property to implement adequate governance and controls around regulatory compliance requirements and attended the Property Compliance Forum. The following issue was highlighted at the last Forum (held on the 13th of August): • the safety certifications have expired for all lifts within the Post Office estate as the assessments have not been carried out by the service provider (Norland). The assessments are the independent means of verification, proving lifts are safe and providing assurance to the regulator and third parties (i.e. Health and Safety Executive) that PO has done everything reasonably possible to ensure lifts are well maintained. The verification exercise has now been approved by PO. Although no detailed formal programme of works has yet been provided by Norland. The verifications are expected to be completed by mid-October. The issues highlighted at the August RCC meeting have not been fully addressed: • Responsibilities to oversee property compliance matters have not been assigned to any GE sub-committee. • The Property Compliance Forum operates without formal Terms of Reference (a draft version has been prepared but still not formally approved and adopted). There is no formal mechanism to escalate the issues and risks identified to a higher management level or committee. • There are no PO dedicated compliance resources providing first line of defence and assurance to mitigate property compliance issues. PO is currently reliant on an interim manager seconded (part time) from Norland, who is technically competent but in no way independent. • There is a need for more rigorous contract management of the services provided by Norland and Servest to ensure expected performance levels are maintained and the necessary compliance is achieved in a timely manner. An initial meeting have been scheduled for the 4th of September between Legal, Internal Audit and Procurement team to discuss how address the above issues.

POL00110129

Overdue actions from audits

	Audit	Action	Assigned to	Forecast Completion Date	Progress
1	**Business continuity**	Prepare and issue BC guidelines to GE / Top management	Corporate Services –Risk Team	Nov 2014	Guidelines are being revised and are subject to he need to test before issue
2	**Business continuity**	Continue negotiations as necessary for recovery desks / options for other key office centres	Corporate Services –Risk Team	Mar 2015	Ongoing as a result of recent BC test issues (Warrington)
3	**Business continuity**	Draw up testing schedule for use as plans are implemented	Corporate Services –Risk Team	Mar 2015	Plans not currently in place, therefore unable to test as yet
4	**Business continuity**	Embed crisis management into the BC process work being carried out across POL	Corporate Services –Risk Team	Dec 2014	Risk team are reviewing the current crisis management processes for rationalisation. Paper to be presented to future RCC
5	**Benefits Realisation**	Finance committee to discuss if and how non financial benefits can be tracked centrally e.g. categories of non financial benefits could be developed and assigned to senior individual across the business.	Finance (Nick Sambridge)	Feb 2015	Whilst the Transformation Design Group will discuss non financial benefits going forwards it is not currently happening. Nick Sambridge has taken an action to recruit someone to focus on this area
6	**Benefits Realisation**	Finance committee to discuss how accountabilities for the delivery of benefits can be enhanced. Eg through the company appraisal / PDR process	Finance	Feb 2015	Finance are awaiting output from OEE consulting review of benefits management – due imminently
7	**Benefits Realisation**	A column will be added to the benefits tracker to show the sources of data used and any assumptions made	Finance – new owner taking over this area	Feb 2015	Update column still needs to be added to Benefits Tracker

POST OFFICE

POL00110129

Overdue actions from audits

	Audit	Action	Assigned to	Forecast Completion Date	Progress
8	LAN – IAM	Management (CIO) have accepted the risk of limited remote access security, taking into consideration the level of change being undertaken in IT. ISAG will perform a risk-costs benefit analysis, based on industry remote access trends.	IT – Roger Middleton	October 2014	The initial control objectives which were intended to be covered by actions 8 and 9 are now to be considered under the deployment of the EUC tower, which includes remote access management and new account creation. The new IAM audit (Q4 in the IA audit plan will be looking at the new controls deployed by EUC tower once in place.
9	LAN - IAM	Controls will be implemented to ensure that new accounts are granted access based upon job description access requirements and appropriate authorisation.	IT – Roger Middleton	Apr 2015	Refer to 8 above

POST OFFICE

POL00110129

Appendix 1 – Contact Management

POL00110129

Contract Management

Internal Audit Report

August 2015

Executive Responsible:	Alisdair Cameron	Prepared By:	Deana Herley – Internal Audit Manager
Distribution:	Jim Rawlings	Reviewed By:	Garry Hooton – Acting Head of Internal Audit Jane MacLeod Jim Rawlings Phil Nedeljkovic

POL00110129

Audit Highlights

Background

The management of supplier contracts within PO is split between the Procurement team and business area that benefits from the relevant service. For IT contracts some elements of contract management are undertaken by Atos.

The objective of the review was to assess the adequacy and effectiveness of current processes and controls over contract management with a specific focus on managing supplier performance.

** There have been some changes to management during the review with leads for both non-IT and IT contracts leaving PO in December (non-IT) and March (IT). The Bravo (portfolio management tool) Administrator also left PO in February 2015, under Wave 1 - Business Transformation. The Purchasing Director and Governance, Systems and Reporting Manager have been appointed post review. Actions have been re-agreed with management as a result.*

Assessment

The findings of our work reveal long-standing and significant issues in the management of non-IT contracts. The root cause of the number of findings is thought to result from the Contract Management Framework (which provides standard operating processes) not being fully developed, finalised and implemented.

The report has three overarching messages on contract management at PO:

1. The split of roles and responsibilities between Procurement and the business is not clearly understood or communicated.
2. PO does not fully recognise and understand the different risks and complexity attached to different types of contracts.
3. PO contract portfolio is not fully known at present.

Whilst it is acknowledged that the focus of Procurement has been on the Town Hall cost saving targets, it is our assessment that there is the risk that the lack of focus on 'business-as-usual' contract management has brought its own associated costs.

(Refer to Appendix A for PWC's suggested Best Practice Framework)

Key issues

1. *Supplier contract portfolio is not fully known.*
2. *Contract Management Framework (CMF) remains in draft (since its development in 2012) and requires further development, finalisation and implementation.*
3. *Staff have the ability to define their own roles and responsibilities.*
4. *Management are unable to effectively foresee and manage expiration of contracts.*
5. *Analysis and management of risks to drive contract management.*

Priority actions

1. *Updating Bravo information as a matter of urgency.*
2. *Further development, finalisation and implementation of the CMF.*
3. *Review, communication and formal allocation of roles and responsibilities.*
4. *Classification of all active contracts in accordance with the CMF.*
5. *Review of expired and contracts due to expire in the next six months in terms of risk and potential value leakage. All material value contracts are being managed.*

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
1. Policies, procedures and process documentation.							
1.1	**Contract Management Framework**	A review of PO contract management activity was completed by the Best Practice team (Procurement) in 2012. This involved reviewing PO existing portfolio of contracts. The output of the work was an outline Contract Management Framework (CMF). The document has not been fully developed and remains in draft. We noted that the CMF has no overall owner due to the individual who developed it leaving the business in early 2014.	Staff do not act quickly and decisively when making decisions. Lack of recognition over the importance of contract management. PO fails to continuously improve.	**High**	a) The CMF should be reviewed and further developed (where required) and finalised. The document should be approved by Chief Financial Officer. b) The CMF should be assigned an overall owner. c) An implementation plan to support the communication / embedding of the CMF should be developed.	a) The most recent CMF material was produced in 2012 and is far from a comprehensive policy and what does exist (.ppt's and .xlss's) was never implemented. A practical and pragmatic approach to implementing CMF within PO is required. b) We have specified the role of Governance, Systems and Reporting Manager (recruitment of which will commence shortly).	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
						c) The action plan will be agreed with the new Purchasing Director and issued (end October, 2015).	
1.2	**Templates**	Templates for elements of the CMF have been developed (completed as a part the activity in 2012). The location of the templates is not clearly understood by staff (held on a local drive) and they are not mandatory in their application. We found that templates are held on a local drive (individual has not left PO) and remain in draft. Testing found they had only been used in one of 10 contracts sampled. This lack of take up is likely to have contributed to the high degree of variation in contract management activity observed during testing.	Inconsistent working practices may lead to inefficiencies, duplication and gaps in control.	**Medium**	Templates should mandate a standard application of processes to ensure consistency and efficiency of approach. Consideration should be given to ensuring that: • storage is centralised and they are accessible to everyone. • they are flexible enough to be proportionate to value and risks of each contract. • are streamlined to clearly show the 'must do's'. • address the Atos on- boarding element.	See response to 1.1	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
1.3	**Business guidance**	Non-IT contracts which are not classified as 'critical' or 'strategic' are currently managed by the business area which benefit from the contract. Management from Procurement have recognised from experience that the business does not have (in the majority of cases) the commercial skills or knowledge to ensure effective and efficient contract management. With this in mind, business owners need the support and guidance of Procurement to ensure contract management activities are carried out as required. This guidance is not available to those individuals and this is partly due to the lack of CMF.	The business has strong technical / operational skills, built through years of experience; however it has currently un-leveraged commercial skills which could lead to value leakage on contracts.	**Medium**	The CMF should incorporate business owner guidance *(including roles and responsibilities)* to ensure those individuals responsible for day-to-day, contract management activities are carried out as required.	See response to 1.1	Governance, Systems and Reporting Manager Action Plan – October 2015
1.4	**Classification of contracts**	The criteria required by the CMF to classify PO contracts as Critical, *Strategic*, *Acquisition* or *Leverage* is not clearly	Contract management activities are ineffective, over engineered	**High**	a) Contracts should be classified using clearly defined criteria and consistent	See response to 1.1	Governance, Systems and Reporting Manager

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		defined, inconsistently applied and, once assigned is not re-assessed on a regular basis.	and/or do not focus on areas of most risk or potential benefit to PO.		terminology, in accordance with the CMF. b) The following should be considered to strengthen overall arrangements: • whether classifications consider the level of risk and complexity of a contract. • the meaning of classifications for Service Delivery and Atos teams to inform the contract management approach. • a single definition and clear approach for each classification. • benefit of reviewing the classification at least annually as a		Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
					part of on-going review of the contract.		
2. Definition of roles and responsibilities of Procurement, Business and ATOS.							
2.1	**Allocation and documentation**	There is no clear allocation of the roles and responsibilities with regard to contract management activity from Sourcing handover through to contract continuance (extension / retender) or exit stages. Issues with individuals understanding their own and others roles and responsibilities were apparent in all contracts sampled with no Atos involvement.	Key contract management activities could fall through the gaps between roles and teams. Issues may not be resolved in a timely manner and opportunities to mitigate risks and optimise services are missed. This may also have a negative impact on PO financially.	**Medium**	a) Roles and responsibilities across the contract management lifecycle should be reviewed. b) An assessment should be carried out over the efficiency and effectiveness, with which roles, responsibilities and accountabilities for contract management activity are delegated throughout PO.	This is a potential issue that will be addressed by the appointment of the new role set out in 1.1 above.	Governance, Systems and Reporting Manager Action Plan – October 2015
2.2	**Handover**	A lack of knowledge transfer and staff continuity between procurement lifecycle phases has been an issue on some contracts. This was evident during sample testing on contracts such as, Capita and Key Property	Key contract management activities may not be completed.	**Medium**	a) Contracts should be reassigned where the Contract Manager assigned on Bravo has left PO. Confirmation should be sent by the relevant	a) All Non-IT contracts are now assigned to the correct Category Manager in Bravo. b) Will be addressed as per the	a) Complete b-c) Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		Solutions. The observed reasons for this include: • *Contract Managers leaving PO without adequate handover.* • *Lack of formalised process for handover and tendering documents not being loaded onto Bravo.* • *Whilst a template has been developed to support the handover process, our testing found that it was not being used by Contract Managers.* • *Contracts are assigned to individuals on Bravo (30%) that have left PO.*			Category Manager (non-IT) and Sourcing Manager (IT) with an agreed deadline for completion. b) Handover processes to transfer responsibilities on Bravo should be clear when: • the named 'Contract Manager' or business owner leaves PO. • A contract becomes active. c) Bravo maintenance responsibilities should be delegated e.g. Category Manager (non-IT) and Sourcing Manager (IT).	response to 1.1 above. c) Agreed and Non-IT team have been instructed accordingly. The broader issue will be addressed as per the response to 1.1.above	
2.3	**Business owner**	The business owner for the contract is not currently captured i.e. not listed or named on Bravo. There is no field	Responsibilities in managing contracts could be unclear or missed through	**Medium**	a) A record listing the business owner against contract should be developed.	a) Practically this is very difficult because the business	Governance, Systems and Reporting Manager

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		on Bravo to enter this. This information is particularly important when Procurement does not actively manage the contract.	a lack of accountability or ownership.		b) Responsibility for ensuring the record is kept up-to-date should be delegated. c) Bravo functionality to support this exercise should be explored.	stakeholders can be many and can change often. The broader issue will be addressed as per the response to 1.1.above b/c) A pragmatic solution needs to be developed once the new role is recruited	Action Plan – October 2015
2.4	**Customer contract management**	Procurement currently has no involvement in the business-as-usual management of in-flight customer contracts (third parties). The focus of contract management for Procurement has been directed towards suppliers. The potential gap in commercial thinking and challenge offered by Procurement could be a missed opportunity for PO.	The best commercial value from the contract during the life of the contract may not be achieved.	**Medium**	The benefits of involving of Procurement in the business-as-usual management of in-flight customer contracts (third parties) should be considered.	Agreed and whilst we are informally engaged in some areas of FS, I am happy to discuss how we engage more formally in the process with other groups.	Jim Rawlings 30 September 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
2.5	**Executive involvement**	The most important, high risk and complex contracts are not formally assigned an Executive owner to drive supplier performance.	Formalised executive owner involvement within contract management could be a missed opportunity for PO.	**Low**	The benefits (e.g. service performance) of formalised Executive owner involvement within contract management activity for the most important, high risk and complex service performance should be considered.	Agree and this needs to be incorporated into PO's supplier management governance model. A pragmatic solution needs to be developed once the new role is recruited.	Governance, Systems and Reporting Manager Action Plan – October 2015
3. **Contract administration.**							
3.1	**Bravo**	For accuracy the contract status in Bravo must be correct i.e. Created (Sourcing), Active (Live) or Expired (Exit, Extension or Retender). As at November 2014, according to the management information from Bravo, PO contract portfolio totalled: 77 Active and 19 Expired	Created contracts on Bravo which are expired (or due to expire) are not captured within the management information. Invoices raised will be based on	**High**	a) Contract Managers should be requested to complete the following actions within an agreed deadline: • ensure the status of their respective contracts on Bravo is correct. • check expiry date	a) All contracts that should be classified as 'Active' now are and have correct end dates. b) Whether or not this functionality can be added Non-IT	a) Complete b) Governance, Systems and Reporting Manager Action Plan – October 2015 c) Complete d) Jim Rawlings 30 September

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		contracts. However, we found the management information generated from Bravo used by the Procurement teams to be inaccurate. This was due to Bravo being inconsistently used by staff (i.e. Contract Managers had not in all instances been changing the contract status from Created to Active in Bravo once live). Of the Created contracts on Bravo, 111 contracts had expired. For 52 expired contracts with a Created status, we found that payments had been made to a significant number of those suppliers after the expiry date. This could be due to various reasons: • Contract has expired. • Expired contract has been replaced, but remains on Bravo. • Bravo has no 'deactivated' status. • New contract has not been uploaded on Bravo.	rates within the expired contracts. Therefore, PO may not get the most competitive rates and billing mechanisms, given time methods move on and these changes will not be reflected by operating under expired contracts. PO is currently unable to effectively foresee and manage expiration so that contractual arrangements can be revisited, closed or updated on a timely basis.		of contract is entered. • where contracts are being managed offline create a record on Bravo. • a confirmation email of actions completed sent to the System Administrator for Bravo. b) Contract 'de-active' status on Bravo should be added if the functionality allows for this. c) Bravo System Administrator should generate management information for the Sourcing Council on: • expired contracts, including date. • contracts due to expire in the next 6 months. d) Bravo entries recorded as:	Category Managers are requesting he Bravo administrator to 'Archive' all contracts that are no longer 'Active' or are no longer valid for whatever reason. c) This was performed and actioned in March, 2015. d) PN will validate whether these still exist.	2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
					'expired contract – catch all vendors' should be reviewed.		
3.2	**Direct Awards**	A 'Direct Awards' paper was presented to the Sourcing Council on 19 February 2014. At the meeting a total contract award of £29 million was approved for 12 contracts to the previous Royal Mail Group (RMG) suppliers following separation. The value was based on contract duration of 18 months. The paper mentioned that re-tendering exercises would be subsequently run on an individual case-by-case basis to capture maximum procurement value for the business. No action plan to support the re-tender exercises has been developed to date. The 18 months is due to expire in September this year.	Delays in the contract award leading to value leakage, given that no value benefits are currently being realised by PO. The opportunity to realise cost reduction / increased value or exit at the earliest opportunity may be missed.	**High**	a) A review of retender requirements (including associated risk / potential value leakage) for contracts as per the 'Direct Awards' paper presented to Souring on 19 February 2014 should be performed. b) An Action Plan documenting the next steps should be subsequently prepared.	A response has been prepared for each and every contract set out within the Direct Award paper.	Complete
3.3	**Retention and management of contractual documentation**	The lack of formal guidance on the retention and management of contractual records has	Suppliers could claim that an electronic copy of the contract has been	**Medium**	A review of PO documentation / data management policies to ensure they are appropriate	We are in the process of verifying now that Bravo has been brought up	Jim Rawlings 30 September 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		led to hardcopy contracts are being stored inconsistently (e.g. Contract Managers, Business Users, Company Secretary and archiving). The location of the hardcopy contract was unknown in 40% of suppliers sampled. Anecdotal evidence from interviews with Contract Managers also suggests that some contracts are being managed offline and therefore have no Bravo system record. A reconciliation between suppliers paid, against Bravo system records indicates that this is likely to be the case.	doctored. Contract could be lost or misappropriated.		and applied consistently across contact management. If necessary, specific policies and procedures should be developed and communicated for contract management. This should cover: • Storage /archiving of hardcopy contracts; and • Retention periods. On completion the existing hardcopy contracts should be stored to this effect.	to date.	
3.4	**Review of contracts**	The accountability for the on-going review of the contract (e.g. quality of service, delivery, adherence to contractual requirements, relationship and value etc.) is unclear at present. There is no formalised timetable or review process agreed. Sample testing found no evidence of review on	Contracts do not meet the evolving business needs. Potential cost saving opportunities in contract being missed by PO.	**Medium**	A process should be put in place for planning and coordinating the on-going review of contract.	Major contracts are being actively managed. A governance process is required. See response to 1.1 above.	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		four of five non-IT contracts sampled. In these instances the contracts had expired. Whilst a Town Hall with suppliers was recently held, which involved review the value of all contracts and identify cost saving opportunities, this should not be a one off exercise.					
4. Supplier performance management including SLA, KPIs and service credits, validation, escalation and resolution of issues.							
4.1	**Supplier self-reporting**	PO relies on supplier self-reporting of performance in the majority of cases. We identified some instances during our sample testing where there was limited challenge to performance reported by suppliers. Whilst it was found that there are some ad-hoc or one-off assurance activities which occur informally on some contracts, this is only on a silo basis. This could be partly due to the lack of CMF to formalise the process for seeking assurance.	Supplier poor performance or inaccurate reporting remains unknown. Performance penalties are not being correctly applied. Payments are made to suppliers for services that have not been delivered.	**Medium**	a) Self-reporting of performance maybe an appropriate to performance measurement in some cases. However the appropriateness should be determined by associated risks, complexity and type of data being reported by the supplier. b) Where processes are identified as 'high risk' through risk assessment, PO	See response to 1.1 above.	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		Sample testing identified there was no Service Level Agreement drafted for the Mindshare contract. We noted that there was some confusion from the business over who was responsible for developing this.			should consider the value of collecting its own performance data in order to independently measure and validate data. c) Procurement should make a recommendation to the Business Owner on whether a Service Level Agreement (SLA) is required during Sourcing. If this is not completed, prior to contract signature or a decision is taken by the Business Owner not take forward, then this should be reflected in the relevant local risk register.		
5. Contractual and supplier risk management.							
5.1	**Risk Management**	Guidance on how risk and issues should be documented, escalated etc. has been developed (back in 2012); however	Risks and issues may not be identified, fully recognised and understood by	**Medium**	a) Contractual and supplier risk management processes should be aligned to the	See response to 1.1	Governance, Systems and Reporting Manager

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		it has not been shared with the relevant business owner responsible risk management. The impact of this was observed in the absence of risk management on PO non-IT contracts. No risk registers had been developed for any of the non-IT contracts sampled instances.	PO, in terms of the different risks attached to the different types of contracts and suppliers.		overall corporate risk management approach for PO and clearly communicated. b) Risks should be actively managed to ensure that controls are in place for mitigation and on-going monitoring. c) Assurance should be planned against the risk dependent on risk rating.		Action Plan – October 2015
6. Management information and reporting.							
6.1	**Continuance Decision Making**	The timing of the continuance decision needs to be such that PO is in a position where it ideally does not operate expired contracts. Feedback from some of the contract management community suggests that the six month trigger on Bravo does not usually give adequate time for a retender exercise to be completed. This has led to behaviours observed such as, extending	Suppliers could potentially complete trading arrangements without effective renewal which could lead to other business or operational issues.	**Medium**	a) The decision making process for contract continuance (exit, extension or retender) should be reviewed. b) The responsibility for monitoring contract expiry / triggering the process should be delegated.	As part of the CMF we will establish variable notice periods for contract expiry according to the time it would take to undertake a re-tendering exercise.	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		contracts due to lack of time and resource to retender.					
7. Atos							
7.1	**Atos.**	The Atos contract is currently being stabilised. A review of the contract by Procurement is due to be completed in April 2015. We observed: • There is a lack of certainty over whether PO is correctly paying for Atos services. This is primarily due to the complexity of the contract (i.e. obligations, costs were written around an integration model with 4 towers). The Contract Manager for Atos is currently pulling together a more detailed overview of Atos obligations. • There is no 'Assurance Plan' for the Atos contract. • Atos operationally holds a risk register for each supplier on-boarded. Risks which have been dealt with by Atos and therefore closed are	The new IT environment fails to deliver the expected benefits e.g. cost savings, risks and efficiencies compared with current environment.	**Medium**	a) A timescale for review of the Atos contract (including detailed view of obligations) should be agreed. b) The assurance requirements for the Atos contract should be determined. c) PO should reconsider the decision not to have visibility over risks dealt with by Atos and therefore closed.	IT Procurement issue. See response to 1.1 (IT Procurement should not work to a different governance process than Non-IT).	Governance, Systems and Reporting Manager Action Plan – October 2015

POL00110129

CONTRACT MANAGEMENT

Ref	Area Reviewed	Findings	Risk	Priority	Agreed Action	Management Response	Owner Date
		currently not shared with PO.					

POL00110129

APPENDIX A – PWC Framework

Best Practice

A mature contract management control environment is based on a formal framework which all personnel involved in contract management are aware of, understand and follow in the sourcing, procuring, managing and operating of contracts. A framework should include the following:

Categorisation of contracts	This allows flexibility across different contracts dependent on the size, risk, value and complexity of a contract arrangement. Each category is subject to different levels of oversight with the most basic contracts requiring very minor on-going monitoring and the more complex contracts requiring more regular and detailed monitoring, independent assurance and collaboration across the organisation.
Roles and responsibilities	These should be clearly defined within the framework. It should be clear who is accountable for what and individuals should be incentivised accordingly (e.g. fixed reward or variable).
Clear linkage between procurement and the business function	The individuals responsible for the operation of the contract should be involved in agreeing the scope, Service Level Agreements and KPIs set within the contract as they will be responsible for managing the contract once in operation. At the very least there should be a formal handover from procurement to the business function.
Clear plan for renewing/renegotiating contracts on expiry	Depending on the length and complexity of a contract it can take a number of months to renew/tender a contract. Trigger dates should exist for all contracts for this process to begin to avoid operating expired contracts.
Minimum management information requirements	A minimum level of management information should be defined up front and be maintained for each contract (the level of which will depend on the categorisation of the contract) as this allows for consistency across contract management.

POL00110129

RCC 7 SEPTEMBER 2015 PAPER EIGHT

Post Office Ltd – Confidential

Risk and Compliance Committee (R&CC)		**Reference: R&CC August 15**
Date: 06 August 2015	**Venue: Boardroom, Finsbury Dials**	**Time: 14:00 – 16:00**
Attending:		
Jane MacLeod (JM)	General Counsel	Chair
Alisdair Cameron (AC)	Chief Financial Officer	Member
Nick Kennett (NK)	Financial Services Director	Member
Paula Vennells (PV)	Chief Executive Officer	Member (Items 1 – 7)
Alwen Lyons (AL)	Company Secretary	Member
Neil Hayward (NH)	Group People Director	Member (Items 1 – 8)
Steve Miller (SM)	Head of Risk	Report
Georgina Blair	Risk Manager	Minutes
Garry Hooton (GH)	Head of Internal Audit	Report
Martin George (MG)	Commercial Director	Report (Item 7)
Andy Garner (AG)	Head of Managed Services	Report (Item 7)
Andy Phillips (AP)	Graduate Trainee, Commercial	Report (Item 7)
John Scott (JS)	Head of Security	Report (Item 8)
Mike Morley-Fletcher (MMF)	Head of Risk and Audit	Guest
Apologies:		
None		

The Chair declared the committee quorate and opened the meeting.

Agenda Item 1, Committee minutes and matters arising

Action 1667 (refresh the gifts and hospitality process with Commercial) was discussed and SM confirmed that the risk team were in the process of reminding the Commercial team of the requirements. NK queried why the action was confined to Commercial and was reminded that the Gifts and Hospitality report at the last meeting had shown very few reports from Commercial.

Action 1666 (present the Conduct Risk Audit to the Committee) had not in fact been closed, as a timing issue meant the papers were not cleared in time to be presented to the meeting. The audit will be presented at the September meeting.

For Action 1660 (clarify Business Transformation reporting line for risk and assurance) JM noted that there were regular BT risk workshops but that these were not governance meetings, and it had been agreed with the Transformation Director that transformation risks would be presented to the RCC as a regular item from October onwards.

For Action 1657 (POMS reporting at RCC) JM confirmed that going forward POMS RCC minutes would be presented to the POL RCC (see item 2) and noted that POMS ARC papers would be presented to the POL ARC.

The committee agreed the minutes of the previous meeting and the attached actions.

Agenda Item 2, POMS RCC minutes and actions

The committee asked NK whether there were any concerns arising as a result of the Collinsons audit. NK noted that POMS had recently undergone a series of audits which had generally shown that it was in good order, despite having only recently been established.

JM asked if the approach to customer detriment was the same in POL and POMS, and NK confirmed that as customer delivery is managed through POL the approach is the same.

POL00110129

NK clarified that POMS has regulatory authority and responsibility for online and telephone sales at present but does not commence oversight of sales within POL branches until 1st October.

AC noted that the style of minute taking in the POMS minutes was more detailed than in the POL RCC meeting, and wondered if this created a risk of recording something that might be taken out of context at a later date. The Committee discussed the more comprehensive style of minute taking required by a regulatory authority and JM noted that the FCA would be looking for evidence of challenge to be demonstrated in the meeting. The Committee requested that JM speak to Victoria Moss to stress importance of capturing this in the POMS RCC minutes (**Action 1668**).

Agenda Item 3, Risk profile update

SM presented the updated risk profile, which included a method of comparing POL's stated risk appetite to the risk exposure of each top risk. This enabled the Committee to consider whether the level of risk exposure was in line with the amount of risk the business was comfortable taking. Incidents and metrics were used to demonstrate whether the qualitative evaluation of risk exposure (the risk score) was correct. The Committee discussed the report and agreed that it was a good start and that work should continue to improve the articulation of controls, and the quality and number of metrics and incidents. It was agreed that SM would engage with Committee members to gain their feedback on the top risks prior to presentation of the revised risk profile in the September meeting (**Action 1669**).

PV queried why Sparrow was not included in the list of the top risks and it was agreed that there would be a separate discussion with JM to determine the appropriate treatment for Sparrow (**Action 1670**).

Agenda Item 4, Risk incidents

The Committee was asked to note the examples contained in these papers as further detail on incidents as mentioned in the risk profile update.

Agenda Item 5, Business continuity planning – status and action plan

SM gave an update on the current status of business continuity planning in the business. The Committee discussed the situation and agreed that there was both a need to understand POL's business continuity landscape in order to identify the gaps, and to test and improve business continuity arrangements on existing key systems.

JM explained that there is no existing resource in the business who can do this (the business continuity function is currently being backfilled by a risk business partner who is spending most of his time on business continuity elements in current procurement processes). JM agreed to determine the scope of the task and estimate the cost and then discuss with AC (**Action 1671**).

The Committee noted that it was likely that there were existing business continuity processes in place covering key systems used in customer critical functions such as Supply Chain and the call centres. PV requested that the key systems were identified and the relevant SLT members asked if they were confident that business continuity arrangements were in place (**Action 1672**).

Agenda Item 6, Incident management process – update

SM briefly explained that there was no single POL-wide incident management process but instead a series of disparate reporting lines, and that further work was needed to identify the optimum solution for POL. The Committee approved the suggested next steps which include a report to the September RCC (**Action 1673**).

Agenda Item 7, Elderly and vulnerable customers review – update

MG and AP updated the Committee on the work that had been done on POL's approach to elderly

POL00110129

and vulnerable customers since the last Committee meeting. This had included a review of the existing processes and procedures in place and identification of the gaps. It had been discovered that a Disability and Discrimination working group had been established and it was proposed that the vulnerable customer work would include their input.

The Committee discussed the definition of vulnerable customers, and recommended that the word 'elderly' was dropped from the description, as not all elderly customers are vulnerable, nor all vulnerable customers elderly. It was noted that it was sometimes challenging to identify vulnerable customers, particularly in the case of temporary vulnerability such as bereavement. AC requested that the costs of any proposed initiatives be reported.

MG agreed to provide a one page update to each successive Committee meeting until this work is completed (**Action 1674**).

PV requested that MG identify the most common sensitive situations where vulnerable customers were encountered (for example, an elderly person whose phone line has developed a fault, or a customer whose relative has died) and ensure that special arrangements were in place and had been communicated to the relevant staff. A short summary of this activity should be provided to the next meeting (**Action 1675**).

Agenda Item 8, AML Annual report

JS provided the Committee with key highlights from the Anti-Money Laundering (AML) report.

It had been identified that up to 2% of branch transactions exceeded the 15,000 Euro limit imposed by POL's class of registration with HMRC. A top-performing branch was currently being investigated for performing transactions above permitted limits and the Committee agreed that it was important that correct action was taken with regard to the agent who had failed to follow the required procedure. The Committee discussed whether POL should consider offering higher value transactions; JM explained that a higher value of transaction brought more onerous customer due diligence requirements and any proposal would need to take this into account. JS explained that the 4th Anti-Money Laundering Directive will reduce the Euro limit to 10,000 Euros and the Committee noted that this is a relatively small amount. JS explained that HMRC was concerned because we cannot track customer spending between different branches.

JS also explained that HMRC were suggesting that POL has ownership and liability for AML matters relating to bill payments on six of our bill payment clients, because of the structure of the contracts.

The Committee discussed the potential mismatch between the contractual responsibility for AML which lies with our banking partners, and the regulatory expectation that we will be carrying out appropriate monitoring and training.

JS explained that there was currently no dedicated AML resource at managerial level, although he was recruiting for a band 4 position which was intended to cover both Financial Crime and AML. JM explained that in order to get a clear understanding of what POL's risk and responsibilities were around AML an external review would be commissioned which would, initially, be funded from the legal budget.

JS mentioned that they were also looking at possible technological solutions to help with monitoring, and the Committee recommended that this be discussed with the Back Office programme. NK asked JS to meet him and Jono Hill to discuss forex and bill payment issues (**Action 1676**).

Agenda Item 9, Internal Audit Report

GH updated the Committee on recent audit activity.

With regard to contract management, the Committee requested that a list of the big contacts and

POL00110129

those responsible for them be produced (**Action 1677**).

The Committee also requested clarification of the assurance programme over IT transformation (**Action 1678**).

Agenda Item 10, Any other business

JM proposed that David Hussey, Transformation Director, be co-opted on to the Committee. The Committee agreed (**Action 1679**) and asked whether there should be someone from Network present. JM said she would discuss Network representation with Kevin Gilliland (**Action 1680**).

JM stated that the rolling agenda would be reviewed at the September meeting.

POL00110129

RCC 7 SEPTEMBER 2015 PAPER EIGHT

Post Office Ltd – Confidential

Action Summary and Updates					
Date	**Ref**	**Action**	**Lead**	**By**	**Update**
08/15	1680	Discuss Network representation on the RCC with Kevin Gilliland, Network Director	Jane MacLeod	7 Sept	Kevin Gilliland or Network representative to attend on 7 September – closed.
08/15	1679	Co-opt Transformation Director onto Committee	Jane MacLeod	7 Sept	David Hussey to attend on 7 September – closed.
08/15	1678	Provide the Committee with clarification of the assurance programme over IT transformation	Garry Hooton	7 Sept	Included in agenda item 7 (Internal Audit report)- closed.
08/15	1677	Produce a list of the big contracts and those responsible for them	Garry Hooton	7 Sept	List of top contracts by spend obtained from Procurement – closed.
08/15	1676	Meet NK and JH to discuss forex and bill payment issues.	John Scott	7 Sept	Meeting set up for 8 October – closed.
08/15	1675	Identify the most common sensitive situations where vulnerable customers were encountered and ensure that special arrangements are in place and have been communicated to the relevant staff - provide short summary of this activity	Martin George	7 Sept	Summary of activity completed provided – closed.
08/15	1674	Provide a regular short update on Vulnerable Customer approach until this work is completed	Martin George	26 Oct	Next report 26 October.
08/15	1673	Present plan, scope of the work required and resourcing model for POL's Incident Management Process	Steve Miller	7 Sept	Included in agenda item 4 (Business Continuity Planning & management) - closed.
08/15	1672	Identify key systems and operations and ask SLT members if they are confident that business continuity arrangements are in place	Steve Miller	7 Sept	Included in agenda item 4 (Business Continuity Planning & management) – closed.
08/15	1671	Scope business continuity resource needed and estimate the cost and discuss with Alisdair Cameron	Jane MacLeod	7 Sept	Included in agenda item 4 (Business Continuity Planning & management) – closed.
08/15	1670	Determine the appropriate treatment (risk or issue) for Sparrow	Jane MacLeod	7 Sept	Reputational risk to be included in POL's risk register, which incorporates the impact of Sparrow – closed.
08/15	1669	Gain feedback from Committee members on top risks prior to presentation of the revised risk profile	Steve Miller	7 Sept	Completed in preparation for Risk Champions Meeting on 19 August – closed.
08/15	1668	Speak to Victoria Moss to stress importance of	Jane MacLeod	7 Sept	

POL00110129

Post Office Ltd – Confidential

		capturing evidence of challenge in POMS RCC minutes			
05/15	1667	To refresh Gifts and Hospitality Policy awareness and discuss reporting process with Commercial	Steve Miller	7 Sept	
05/15	1666	Conduct Risk Audit (FS) to be presented to the Committee	Garry Hooton	7 Sept	FS senior management leave commitments meant audit not yet cleared. Due to be cleared in w/c 14/09.
05/15	1663	Corporate governance code 'gaps' and proposal on work to improve compliance for 15/16 ARA to be presented to the Committee in preparation for presentation to the ARC in September and Board in October	Steve Miller	7 Sept	Included in agenda item 3 (Corporate Governance Code & Control Framework).
03/15	1657	Discuss interaction between POL and POMS with regard to reporting at RCC with Financial Services Director	Jane MacLeod	6 August	Done – POMS RCC minutes to be presented to POL RCC – action closed.
01/15	1655	Prepare and implement a communications plan to raise awareness of the whistleblowing line	Steve Miller	26 October	Whistleblowing framework currently under review. Action point carried forward to next meeting.
01/15	1649	Commercial Director to give an update on vulnerable customers- definition and proposed best practice at the next meeting.	Martin George	6 August	Done – see item 7 of August 2015 meeting - action closed.

Next Meeting – 26 October 2015 Room 1.19 Wakefield 12.00 – 14.00

POL00110129

Company no. 8459718 – Strictly Confidential

PR&CC 15/01– 15/07

POST OFFICE MANAGEMENT SERVICES LIMITED (POMS)
RISK & COMPLIANCE COMMITTEE (R&CC)
(a committee of the executive)

Minutes of a POMS R&CC meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 18 August 2015 at 1.30pm

Present:	Nick Kennett (NK)	CEO (Chairman for the meeting)
	Richard James (RJ)	Managing Director (interim)
	Craig Elmer-White (CEW)	Head of Operations, POMS
	Rob Clarkson (RC)	MD Post Office Insurance
	Ben Foat (BF)	Head of Legal Financial Services
	Victoria Moss (VM)	Deputy Company Secretary
	Laurence Rixon (LR)	Project Manager and Business Analyst (Thistle Initiatives Limited)
	Russell Weekes	Head of Compliance (interim)
Apologies:	Colin Stuart (CS)	Head of Commercial Finance

PR&CC 15/01 **QUORUM AND CONFLICTS OF INTEREST**

(a) The Chairman declared the meeting quorate and open.

PR&CC 15/02 **MINUTES OF THE MEETING HELD ON 14TH JULY 2015**

Action: LR, VM

(a) The R&CC discussed the matter of the style of the meeting minutes. VM and LR agreed to liaise to ensure that a uniform style is used for future meetings which reflects the tone of conversations, issues raised, outcomes determined and conclusions given rather than a semi-verbatim style.RW to discuss with VM possibility of a member of the Company Secretariat taking future responsibility for minute taking within the R&CC.

Action: RW

(b)

Action: LR

(c) The R&CC requested that the actions be recorded in way which mirrors the POMs Executive committee style. LR to liaise with VM to arrange this.

POL00110129

PR&CC 15/02 **ACTIONS LIST**

(a) Action point from agenda item three from the minutes of 14th July 2014 meeting - the R&CC discussed a post-implementation review of POMS now that the new branch network sales process has been live for two months. It was suggested that Paul Jones, Head of Travel Insurance (PJ) could be used as a potential resource to conduct this review. RW to discuss with PJ and revert. The review should include data from the contact centre and be linked to Collinsons quarterly review.

Action: RW, RJ

Action: RW (b) Action point five from agenda item four from the minutes of the 14th July 2014 meeting – revision of the report format with claims data reported in arrears to be carried forward to the next meeting

PR&CC 15/03 **R&CC ROLLING AGENDA**

(a) The R&CC members discussed the need for the POMS board to review the policies as suggested by Thistle to the HAWK team. RJ and RW confirmed that the vast majority of these are already in place and it was confirmed that a review of these is scheduled for Sept/Oct 15. The policies themselves were not reviewed during this R&CC session. RW to prepare a document to present at next month's R&CC which details the following:

Action: RW

i. The number of policies which are in place
ii. The number of policies which are outstanding
iii. Which of the policies have been signed off by POMS
iv. Which of the policies have been signed off by Post Office only
v. The status of each policy
vi. List the policies which are required for day one
vii. How many have been changed vs. how many have not been changed from the Post Office versions.

PR&CC 15/04 **Principal Risks**

(a) The R&CC discussed the need to update the actions for each risk as some were outdated. RW to update actions section of the Risk Register

Action: RW

(b) The R&CC discussed the improved risk rating for digital now that the mobile customer journey has been effected. The

POL00110129

R&CC suggested that an additional risk relating to the new directly regulated status should now be included within the risk register. The members considered whether or not POMS will hold a greater risk as the Principal as opposed to being an Appointed Representative. RW to add the new risk into the Risk Register and accompanying document with a view to this to be presented to the Board in September regarding what will it look like under the new regime. RW suggested producing an impact table to demonstrate this and agreed to review this possibility.

Action: RW

(c) The R&CC discussed the ongoing data validation review whereby POMS is seeking to ensure that the management information and reporting produced is accurate.

(d) The R&CC discussed that in the post-HAWK era, POMS is accountable for what the Post Office does and POMS need to be confident that the Post Office is adhering with regulatory requirements. The members then discussed that there are no preventative controls within the Post Office and there is only detective management information. NK and RC suggested that POMS will need a broad understanding of what will be inherited as POMS and what plans we have in place. The members discussed whether a IRRELEVANT IRRELEVANT could be legally applied and whether it would be practical. An example was given as to whether we are able to confirm that those customers that have no medical cover in place are aware of the policy limitations. RW to produce a report which details the position that POMS will be in from 01 October 15 and what plans are in place. As part of the project HAWK completion discussions the POMS Board will be provided with an update at its meeting in September.

Action: RW

PR&CC 15/05 **COMPLIANCE REPORT**

(a) The R&CC discussed the condensed format of the Compliance Report. NK to feedback likes and dislikes within this format to RW for revision.

Action: NK

(b) CEW talked through the Contact Centre and Branch reporting elements and explained that the new Quality Assurance (QA) scorecard would be coming in and will provide a more accurate definition of the risks faced through WebHelp UK (WHUK). The committee members

POL00110129

discussed the relevance of conducting cancellation call audits and it was explained that this is due to the FCA's focus on Post Sale Barriers (PSB) within this area. The members discussed whether there is a risk-based way of measuring PSB's as opposed to auditing a 30% sample now that POMS has moved to being a directly regulated entity. CEW explained that these are conducted to ensure quality and a review of the cancellation code 'dispositions'.

(c) RW discussed his visit to Collinsons and advised that this had identified some internal challenges for the business included gaps in current governance arrangements, lack of a compliance risk assessment being performed for the incoming POMS business and a lack of clear responsibility for decision making in claims handling. RW had reviewed whether or not there was a T&Cs focussed culture in relation to assistance and claims handling and confirmed that he had not identified any real causes for concern. RW confirmed that feedback from Collinsons was that claims volumes were below expectation in June and therefore there may be an influx of calls during July as a result. RW to verify the declined claims vs claim volume data reported as the members queried this in that it was not clear if this was accurate. RW to arrange for 2nd draft of Collinson's/GLUK audit to be sent to NK in time for September as requested.

ACTION: RW

ACTION: RW

PR&CC 15/06 **REGULATORY UPDATE**

(a) RC discussed the FCA's review and focus on insurance add-ons. RW demonstrated the categorisation of sanctions and explained that Dalesridge perform the checks against the Sanction List every Friday and each time a new list is published, the entire POMS book is cross-referenced against it.

PR&CC 15/07 **ANY OTHER BUSINESS**

(a) There being no further business the Chairman declared the meeting closed.

....

Chairman **Date**

POL00110129

RCC 7 SEPTEMBER 2015 PAPER TEN

To: RCC

From: Information Security and Assurance Group (ISAG)

Re: Updated Cyber Security Charter

Purpose:

1. The Risk and Compliance Committee is asked to note this charter, which has been reviewed and updated in line with changes within the business.

Background:

2. For POL's ISO27001 Certification it is a requirement that the business outline their Information Security/Cyber Security strategy and the accountabilities, which is outlined in this updated document.

Emma McGinn
2 September 2015

POL00110129

POST OFFICE CYBER SECURITY & INFORMATION ASSURANCE CHARTER

POL00110129

Document Control

Overview

Owner:	Head of Information Security & Assurance	**Enquiry point:**	ISAG
Version:	0.1	**Effective from:**	
		Last updated:	

Revision History

Version	Date	Author	Changes
0.1	31/07/2015	Claire Davies	Initial Release
0.2	24/08/2015	Emma McGinn	Peer Review

Reviewers

Version	Date	Reviewer	Comments
0.1	03/12/2014	Julie George	Minor amendments to original draft

POL00110129

Executive Summary

Post Office's Board and Group Executive (GE) recognise that Cyber and Information Security threats present significant commercial and operational risk to Post Office and to those of its subsidiaries. GE are committed to developing a strategic response to current and emerging Cyber and Information Security threats as an enabling mechanism for Post Office to achieve its growth, modernisation, customer focus and employee engagement objectives whilst preserving Post Offices' brand, commercial image, reputation, competitive advantage, revenues, and profitability alongside legal, regulatory and contractual compliance.

In response to this, GE have devolved accountability for Cyber and Information Security to the General Counsel and established the Information and Security and Assurance Group (ISAG) who are ultimately responsible for the establishment, implementation, maintenance and continual improvement of Post Office's Cyber Security and Information Assurance (CSIA) framework.

Organisational Structure

General Counsel has devolved responsibility for CSIA to the Head of Information Security and Assurance who is supported by ISAG. Additional CSIA contractors will be recruited and allocated on a needs basis for specific Post Office projects or programmes.

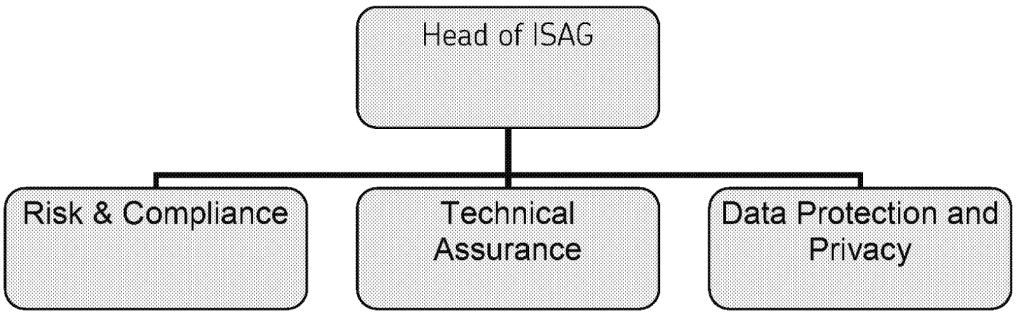


Figure 1: ISAG High Level Structure

Scope

The scope of ISAG includes responsibility for the systemic security governance, risk assessment and compliance oversight across all business areas within Post Office and our third party supply chain. These are generally consistent with the recommendations in the ISO 27002 code of practice and the associated ISO 27001 Information Security Management System standard. Another key benchmark is the PCI-DSS (Payment Card Industry-Data Security Standard).

Responsibilities

The responsibilities of the General Counsel with respect to CSIA are as follows:

- Presentation of CSIA reporting to GE.
- Ensure ISAG is adequately resourced.

POL00110129

The Head of ISAG is to:

- Where CSIA policy and/or standards cannot be met, make information risk decisions on Risk Acceptance Notices in accordance with business risk appetite.
- Build and maintain a professionally competent ISAG, capable of meeting the CSIA needs of Post Office.
- Assume an equivalent accountable Cabinet Office role of the Senior Information Risk Officer (SIRO),
- CSIA reporting to GE via General Counsel.
- Develop the CSIA management framework.
- Establish an Information Security Governance, Risk & Compliance Framework.
- In association with the corporate risk function, deploy an Information Security Risk Management Framework.
- Identify, manage and measure information compliance and privacy requirements.
- Plan for, direct and/or support information audit requirements.
- Develop and maintain CSIA policy set with supporting standards.
- Maintain an overview and assure Security Architecture.
- Provide governance and assurance of Digital Connections
- Manage and deploy intelligence solution for the provision of timely threat intelligence and effective counter measures.
- Management of Information Security and Data Protection incidents.
- Encourage the correct security behaviors throughout the business and deploy annual awareness training.
- CSIA provision within:
    - Identity and Access Management;
    - Vulnerability Management;
    - System Development Management;
    - Asset Management;
    - Change Management;
    - Crisis Management;
    - Business Continuity; and
    - Human Resources.

Due Diligence

Since part of the Post Office's strategy is to multisource / outsource, ISAG involvement is imperative in new programme initiatives including any transformation activities. The ISAG involvement shall be mandated by the inclusion of information security within the Programme Initiation Documentation as a Design Authority contributor. For newly created business activity at the time of the High Level Design creation, Information Security and Assurance Group shall be involved to ensure that they are able to advise and assist at the earliest opportunity to ensure risks are managed appropriately.