POL00333330

Risk & Compliance Committee Meeting
POL Boardroom, 1st Floor, 148 Old Street, London, EC1V 9HQ
20th January 2014, 13.30pm – 15.30pm

Committee
Chris Aujard (Chair)
Paula Vennells
Chris Day
Alwen Lyons

To Attend
Dave Mason
Julie George
Georgina Blair
Jonathan Hill
Rob Bolton

Apologies:

	Agenda Item	Purpose	Timings	Papers	Owner
1.	**Top 10 Business Risks** i) Overview of top 10 risks ii) Focus session on selected risk – FS Mis-selling	**Review and endorse approach**	13.30 – 14.30 60 minutes	**Paper One (Appendices 1 – 5)** **Paper Two** **Paper Two(a)**	Dave Mason Jonathan Hill
2.	**Risk Management Strategy** i) Risk Plans ii) Risk Management Update	**Receive update**	14.30 – 14.45 15 minutes	**Paper Three (Appendix 6)**	Dave Mason
3.	**Stewardship** i) Risk Events and Near Misses ii) Assurance Activity iii) Compliance Reports	**Review and agree recommendations**	14.45 – 15.00 15 minutes	**Paper Four** **Paper Five** **No compliance reports this time**	Dave Mason
4.	**Business Policy Approvals and Framework** i) Statutory Policy Framework ii) Policy Approvals	**Approve policies and endorse approach**	15.00 – 15.20 20 minutes	**Paper Six (Appendix 7)** **Anti-Bribery Policy** **Acceptable Use Policy** **External Data Protection Policy** **Data Sharing Policy**	Dave Mason Georgina Blair Julie George Julie George Julie George
5.	**Committee minutes & matters arising** i) Agree updated meeting minutes of 23rd October ii) Review matters arising from 23rd October	**Agree minutes and review action updates**	15.20 – 15.25 5 minutes	**Paper Seven – Minutes & Actions** **Paper Eight – Action 1552 Update**	All
6.	**Meeting A.O.B** i) NMO		15.25 – 15.30 5 minutes	**Verbal update to be provided at meeting**	Dave Mason

POL00333330

Strictly Confidential **PAPER ONE**

RISK AND COMPLIANCE COMMITTEE

Overview of EXCO risks

1. Purpose

The purpose of this paper is to:

1.1 Update the committee on the approach being taken and progress in documenting the key risks identified by ExCo and presented to the Board.

- This agenda item is intended to be the vehicle through which the Risk and Compliance (R&C) function provides the committee with assurance that these risks are being effectively managed.

- As the first paper of this type, it is written with the intention of gathering the committee's feedback on how the data should be presented in the future. The R&C function expects an on-going dialogue with the committee in this area.

1.2 Seek endorsement from the committee of the "BowTie" approach and methodology summarised in the following section.

2. Approach

2.1 ExCo has identified key risks and the associated impacts and controls which require senior management attention. After the initial analysis by ExCo the risk management function has worked with the risk owners and subject matter experts to further refine the causes, controls and consequences associated with each of the risks.

POL00333330

Strictly Confidential **PAPER ONE**

2.2 We are initially using the risk centred 'bow tie' approach as implemented in many other firms, including both financial services and the public sector:-

- It identifies the relationships between outcomes, causes and consequences;
- The method requires us to specify the outcomes we need to avoid as well as identifying trigger points for such events;
- Controls show what processes we have in place to prevent the causes and mitigate the consequences; and
- We can then identify the actions we need to take to improve control and the measures we need to ensure they are operating effectively.

POL00333330

Strictly Confidential **PAPER ONE**

3. Key Risk Status Summary

The initial development of the "bow ties" has, by necessity, been led by the R&C function. Due to the timing of the effort and the seasonal demands on resources, it has sometimes been a challenge getting the appropriate level of engagement from relevant managers.

Reflecting this, and the varying levels of maturity of existing risk management processes, the first pass analysis of causes, consequences and controls is not yet in place for the majority of the risks. We plan to complete this activity before the next committee meeting.

The following agenda item 1.ii presents the completed analysis of the Financial Services (FS) mis-selling risk. This is our best example of "what good might look like".

The status of the bow tie analysis for each risk is summarised in the table below. Even where noted as complete, each element will be continually refined as understanding increases. Where the draft "bow tie" is available and has been agreed with appropriate stakeholders, it has been included as an appendix.

Risk Description	Owner	Causes Identified	Consequences identified	Controls Identified	Control Measures Identified	Action Plans in place	Appendix
Allegations relating to the integrity of the Horizon system	Chris Aujard	Not required see section 4					
Failure to deliver top line growth in line with strategic plans	Martin George Nick Kennett	In Progress	In Progress	Planned	Planned		1
Operating model fails to deliver requisite cost savings	Chris Day	In Progress	In Progress	Planned	Planned		
Inadequate people capability or capacity to deliver transformation change and the strategic plan	Fay Healey	Complete	Complete	In Progress	In Progress	In Progress	2
Non delivery of Network Transformation programme	Kevin Gilliland	Complete	Complete	In Progress	In Progress	Planned	3
Strike action within supply chain could damage ability to distribute cash to network	Kevin Gilliland	Complete	Complete	In Progress	In Progress	Planned	4
Delivering poor customer outcomes through Financial Services mis-selling	Nick Kennett	Complete	Complete	Complete	Complete	In Progress	
The security & integrity of PO data cannot be maintained	Lesley Sewell	Complete	Complete	Complete	Planned	Planned	5
Cybersecurity	Lesley Sewell	Complete	Complete	Complete	Planned	Planned	
POL cannot operate or deliver services following IT transformation	Lesley Sewell	Complete	Complete	In Progress	In Progress	Planned	

The following section (4) provides more detail for all the risks, including an agreed view of the current management of each risk.

POL00333330

Strictly Confidential **PAPER ONE**

4. Key Risk Status

For each risk we have included:-

- The ExCo Owner of the risk,
- A view of the current state of the management of the risk, agreed by the Risk Owner, and
- The current status of the Bow Tie analysis.

Note: the risk of delivering poor customer outcomes through Financial Services mis-selling is not detailed here as it is the subject of a "deep dive" in the next agenda item (1.ii).

4.1 Allegations relating to the integrity of the Horizon system

ExCo Owner: Chris Aujard

There is a risk that the allegations relating to the integrity of the Horizon system, if not contained, could raise wider questions over the robustness of our core systems and our ability to operate, damaging (amongst other matters) current partnerships, new areas of expansion and public and government confidence.

Current State

This risk has been re-classified as an issue as the allegations have been made. It will be followed up as such.

Two programmes, Sparrow and Business Improvement, have been initiated to address the impact, containment and root cause of the issue.

The R&C team will work with the programme teams to build on initial root cause analysis; this will be mapped against the programme scope to verify that the right actions are being taken to mitigate the risk of future occurrence of this issue.

Sparrow has established governance in place including proactive risk and issue management, with blockers to issue resolution escalated through to the programme board. Risks, Assumptions, Issues and Dependencies (RAID) workshops are held monthly by the programme team and attended by the Risk Business Partner.

The Business Improvement Programme governance model is being revised following agreement to the Terms of Reference.

Bow Tie Status

As this has been determined to be an issue, no Bow Tie document is being produced

POL00333330

4.2 Failure to deliver top line growth in line with strategic plans

ExCo Owner: Martin George & Nick Kennett

Lack of growth in both Financial Services (FS) and across the Commercial portfolio would have a detrimental impact on delivery of the strategic plan. Non delivery of growth targets will reduce the appeal of the franchise model impacting Network Transformation. There is an immediate threat that long term growth targets could become unachievable if we do not respond quickly to competitors.

Current State

Financial Services
Many of the risks inherent in the growth plan are already covered individually within the FS risk register, with owners and controls. However further work is required to develop these risks as well as the assessment of the state of the controls including the use of risk indicators (as for FS mis-selling). Overall the FS growth risk is assessed as 'amber' because it is at an early stage and a number of key enabling projects whilst planned for and 'in progress' still need to be delivered.

An initial draft FS growth risk bow tie is being developed. However, this needs to be refined and reconciled with the MI that is already available from different parts of the business e.g. from Project Status updates.

Commercial
Growth across the Commercial portfolio has hit a number of set-backs – predominantly the failure of Royal Mail to swiftly address the pricing model which led to the "shoe-box" issue and Gov. Services failing to materialise in line with anticipation. Further issues such as the migration issues of fixed line telecoms services have not helped but despite this, the development and launch of the new mobile telecoms service is still on target. The introduction of new project boards to help identify and mitigate emerging project risks should help eliminate any future slippage to strategic projects in development to help grow the business. However, existing MI does require evaluating to assess its effectiveness in monitoring both preventive and detective in order to ensure that swift action to mitigate any risk events takes place (Appendix 1).

Bow Tie Status

Identification of causes and consequences is in progress, control and control measures definition is planned.

POL00333330

Strictly Confidential **PAPER ONE**

4.3 Operating Model fails to deliver requisite cost savings

ExCo Owner: Chris Day

Reduction of costs and sustained cost management are imperative if we are to generate the level of profitability required to make Post Office commercially sustainable. A multi-faceted programme of transformation coupled with challenging growth targets can conflict with a cost reduction programme.

Current State

There are two significant strands to the delivery of requisite cost savings:-

- Improved efficiency within the current operating model. A number of sustainable cost reduction initiatives have been identified, the majority of which are governed through standard business performance management. Those that are on hold, for various reasons, are governed by the cost management task force.

- Strategic cost reduction and business transformation programme. This is a new programme currently in the planning phase, focussing on building the team and preparation for the tender process due to commence in March 2014.

Of the two strands, the strategic cost reduction and business transformation programme carries the most risk and will receive a greater focus by risk management. Governance controls are being established and programme delivery risks are in the process of being identified. Due to the significance and breadth of the programme a full risk workshop with relevant subject matter experts will be facilitated by the Risk and Compliance function (Date TBC). The output of the workshop will be a full identification of the possible casual factors, likely consequences and mitigating controls. Additionally the Risk Business Partner aligned to the Finance directorate will attend regular risk and issue discussions once set up.

Bow Tie Status

Identification of causes and consequences is in progress, control and control measure definition is planned.

POL00333330

4.4 Inadequate people capability or capacity to deliver transformational change and the strategic plan

ExCo Owner: Fay Healey

The capability of our people is critical to successful delivery of all facets of the strategy. There is a risk that we cannot retain, recruit and effectively performance manage our people to the level of capability required within the necessary timeframe. Additionally, as we continue to grow our capability there is a risk that the pool of existing talent is oversubscribed increasing pressure and reducing their effectiveness.

Current State

Initial identification of causes and mitigating controls is complete (Appendix 2). This activity has highlighted the breadth of the risk as well as the significant contribution to other key risks such as failure to deliver top line growth. The risk will continue to be monitored and may need to be expanded, particularly relating to agents. This will be reviewed further following the appointment of the Group People Director.

Good progress has already been made in identifying key control gaps and initiating development activity, including ten Learning and Development (L&D) workstreams, to address these gaps.

Work is underway to build on existing metrics once complete this MI will contribute to the build of appropriate Key Risk Indicators (KRI's) and Key Control Indicators (KCI's)

Whilst ownership of creating the right framework and tools sits firmly within HR, mitigation of the risk is dependent upon all managers across the organisation. The risk is universal and must be acknowledged and owned throughout the organisation.

Bow Tie Status

Identification of causes and consequences is complete, controls and control measures definition is in progress and the development of remedial action plans is in progress.

POL00333330

4.5 Non-delivery of Network Transformation Programme

ExCo Owner: Kevin Gilliland

Failure to deliver network transformation in a timely fashion would result in a non-viable business model requiring additional subsidy from the Government or closure of branches, neither of which are sustainable options. There is an immediate risk that if we do not manage current and prospective partners and stakeholders effectively, we may find that we cannot secure the retail partners we need to secure the future of our network.

Current State

As a result of the recent announcement regarding changes to network strategy, the Network Transformation (NT) Programme is in the process of conducting a thorough review of all risks on its risk register. A number of the previous risks were associated with the voluntary nature of the programme and these are now being removed. New risks exist as a result of the new strategy and the top risks have already been reported and shared with ExCo via the NT Programme Board (Appendix 3). There is substantial management information available for the programme and existing metrics are being reviewed to ensure they align to the revised risks.

Review of this risk has highlighted the breadth of the risk, dependencies on other risks such as inadequate people capability and its significant contribution to other key risks such as failure to deliver top line growth and failure to deliver cost savings. Please note that the Risk, as raised by ExCo, relates to the Network Transformation Programme only and does not cover the Crown Transformation Programme

Bow Tie Status

Identification of causes and consequences is complete, controls and control measures definition is in progress and the development of remedial action plans is planned.

POL00333330

4.6 Strike action within supply chain could damage ability to distribute cash to network (IR/CWU)

ExCo Owner: Kevin Gilliland

Whilst there are multiple controls, and back up plans, in place to mitigate the risk of a breakdown in cash distribution there is a risk that these will be insufficient to deal with a with continued strike action. The impact of branches not receiving the cash they need to serve our most vulnerable customers would be detrimental to the Post Office reputation.

Current State

Initial identification of main causes and mitigating controls is complete (Appendix 4). This activity has highlighted that if this risk materialised it would significantly contribute to other risks, such as the risk of failure to deliver top line growth in line with strategic plans.

Good progress has already been made in identifying key control gaps and initiating mitigation activity; the latter has resulted in a temporary cessation of strikes. Some of the mitigating actions, in particular the contingency planning, have also been successfully tested in the short term during recent industrial action.

This risk will continue to be monitored and the metrics reviewed.

Bow Tie Status

Identification of causes and consequences is complete, controls and control measures definition is in progress and the development of remedial action plans is planned

4.7 Delivering poor customer outcomes through FS mis-selling

ExCo Owner: Nick Kennett

The rate and pace of change in the Financial Services Area, Financial Services has a demanding growth agenda that will require more sales to be generated through a variety of channels particularly in insurance. This includes a number of new projects, product developments and pilots. There is a risk of regulatory failure and client dis-satisfaction through mis-selling by staff or agents

Current State and Bow Tie Status
This risk will be covered in detail in the next agenda item (1.ii).

POL00333330

4.8 The security and integrity of Post Office data cannot be maintained.
4.9 Cybersecurity

ExCo Owner Lesley Sewell

Currently the risk analysis covers both risks together. The next iteration will identify internal and external threats, causes, controls and consequences to allow separate analysis of the two risks.

The integrity and security of Post Office data is reliant on a complex network of interrelated processes and controls. The number of potential threats, particularly of external attacks through the internet, is rapidly increasing.

Current State

The identification of causes, consequences and high level mitigating controls is complete (Appendix 5). Generally, controls are in place to address the causes identified although many are constrained by the limited resources available to the Information Security function. The PCI DSS and ISO 27001 certifications support this conclusion; albeit they have been successfully attained or retained through acceptance by third parties that plans exist to address the resultant risk to the organisation. Some other control gaps have already been identified and escalated.

Effectiveness measures are in place for the majority of controls but the detailed review and identification of Key Control Indicators and Key Risk Indicators would best be done after the implementation of the Service Integrator / Service Desk (SISD) programme as currently there are a number of unknown factors which will need to be assessed.

Bow Tie Status

Identification of causes and consequences and the definition of controls are complete, the development of control measures and remedial action plans are planned.

POL00333330

Strictly Confidential **PAPER ONE**

4.10 POL cannot operate or deliver services following IT Transformation

ExCo Owner Lesley Sewell

The IT Transformation is critical to the delivery of the overall transformation programme and will completely restructure and realign the IT supplier network, introducing ATOS as the service integrator. The various contractual relationships, the multiple components of the programme and the pervasive nature of the changes create a complex and changing risk landscape.

Current State

An initial identification of the causes, consequences and mitigating controls of the IT Transformation risk has been completed. (Further review by programme management is underway) The risk as identified by ExCo refers to the business as usual state after the programme has completed, the review has focussed on the current controls within the programme. Further work will be required to cover post implementation causes and controls in the new environment

Existing controls have been identified that address the potential causes of the principal risk, centred around programme oversight and contract management supported by those to be in place in the retained environment. The programme management process provides multiple performance measures which will be reviewed to ensure they provide adequate measures of control effectiveness.

Bow Tie Status

Identification of causes and consequences is complete, the development of controls and control measures is near completion and the development of remedial action plans is planned.

5. Action

The committee is asked to:-

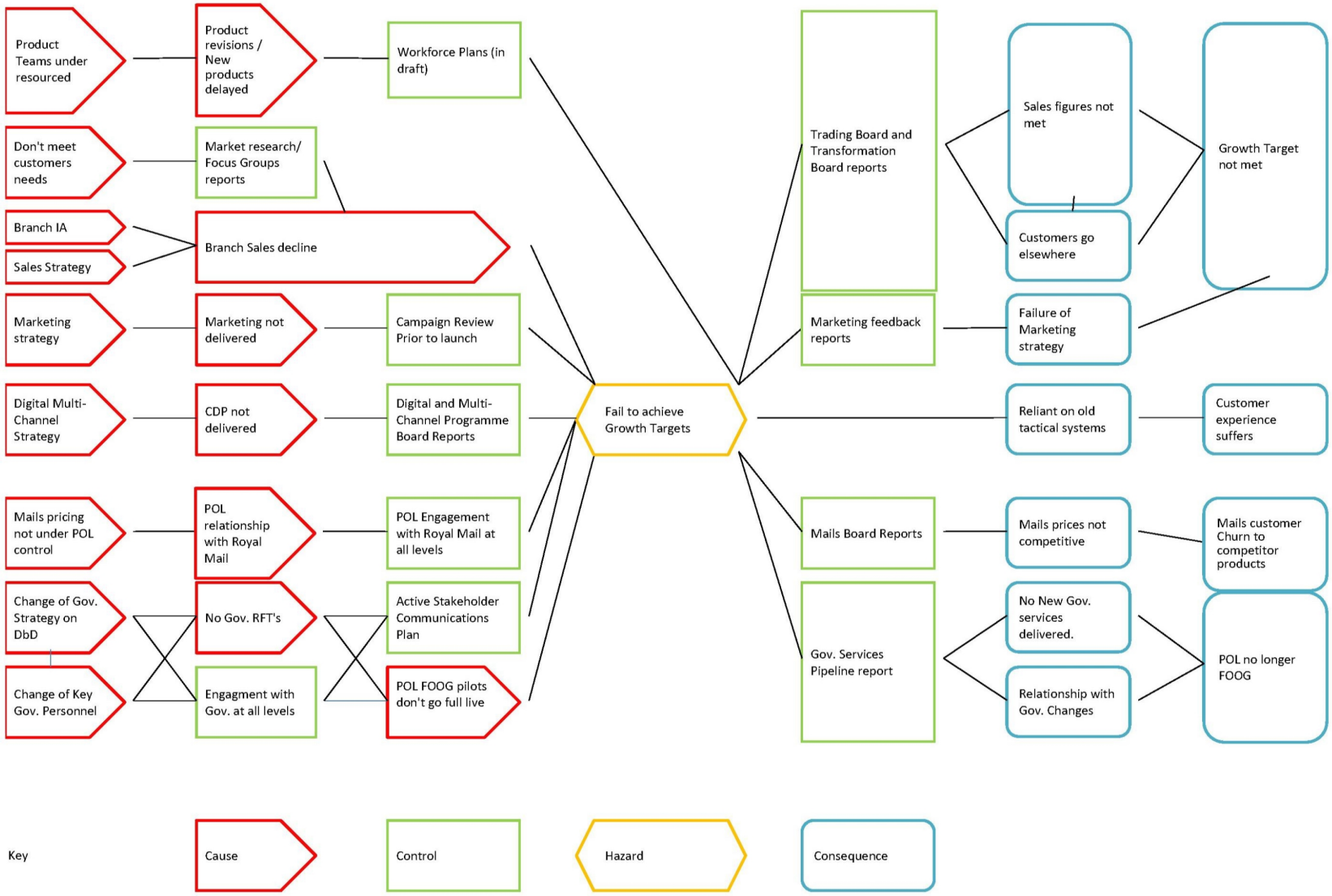
5.1 Endorse the bow tie approach and methodology identified in this paper, and

5.2 Provide feedback on the content and structure of this section for future committees.

Dave Mason
20th January 2014

POL00333330

COMMERCIAL BOW TIE : PAPER ONE APPENDIX 1

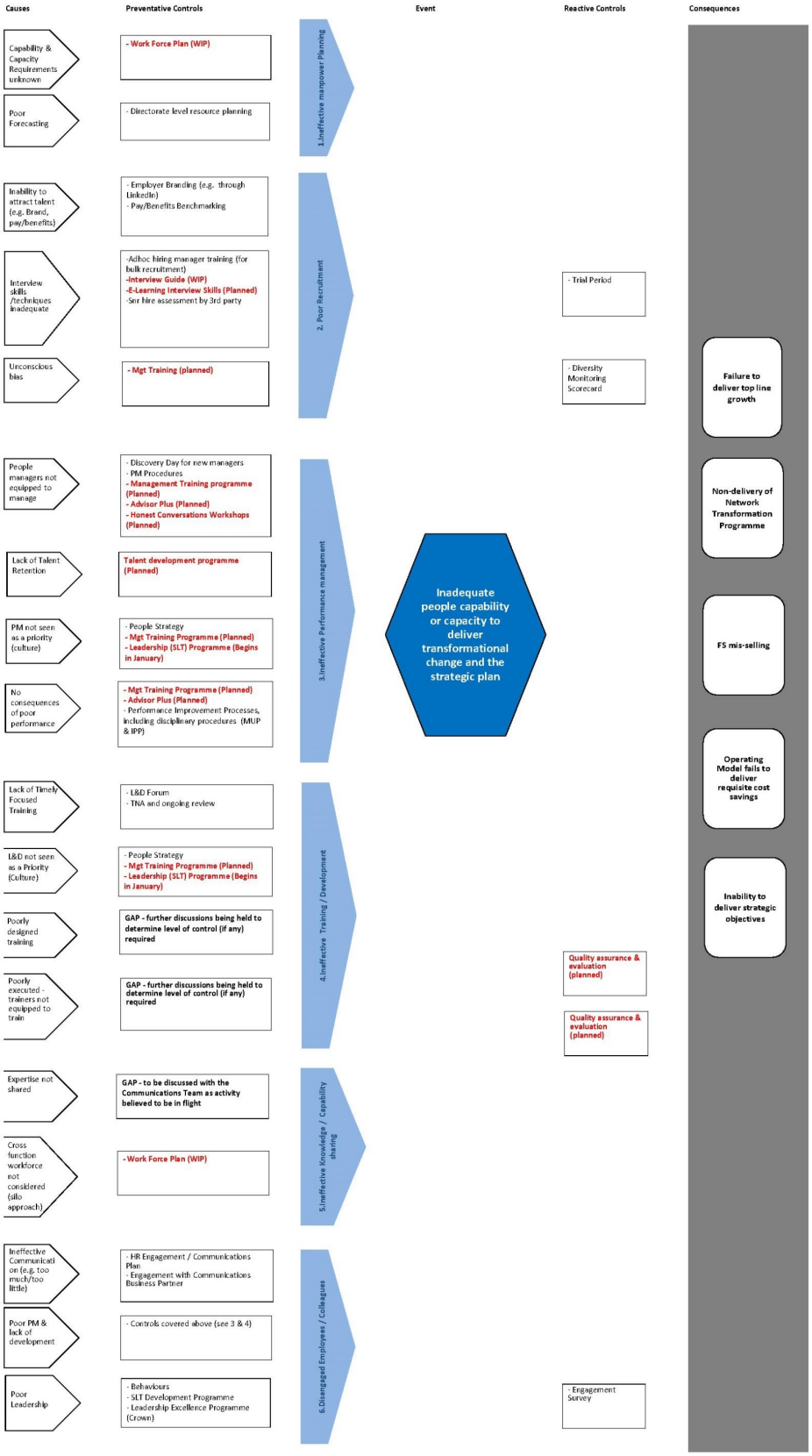


POL00333330

1. Top 10 Business Risks

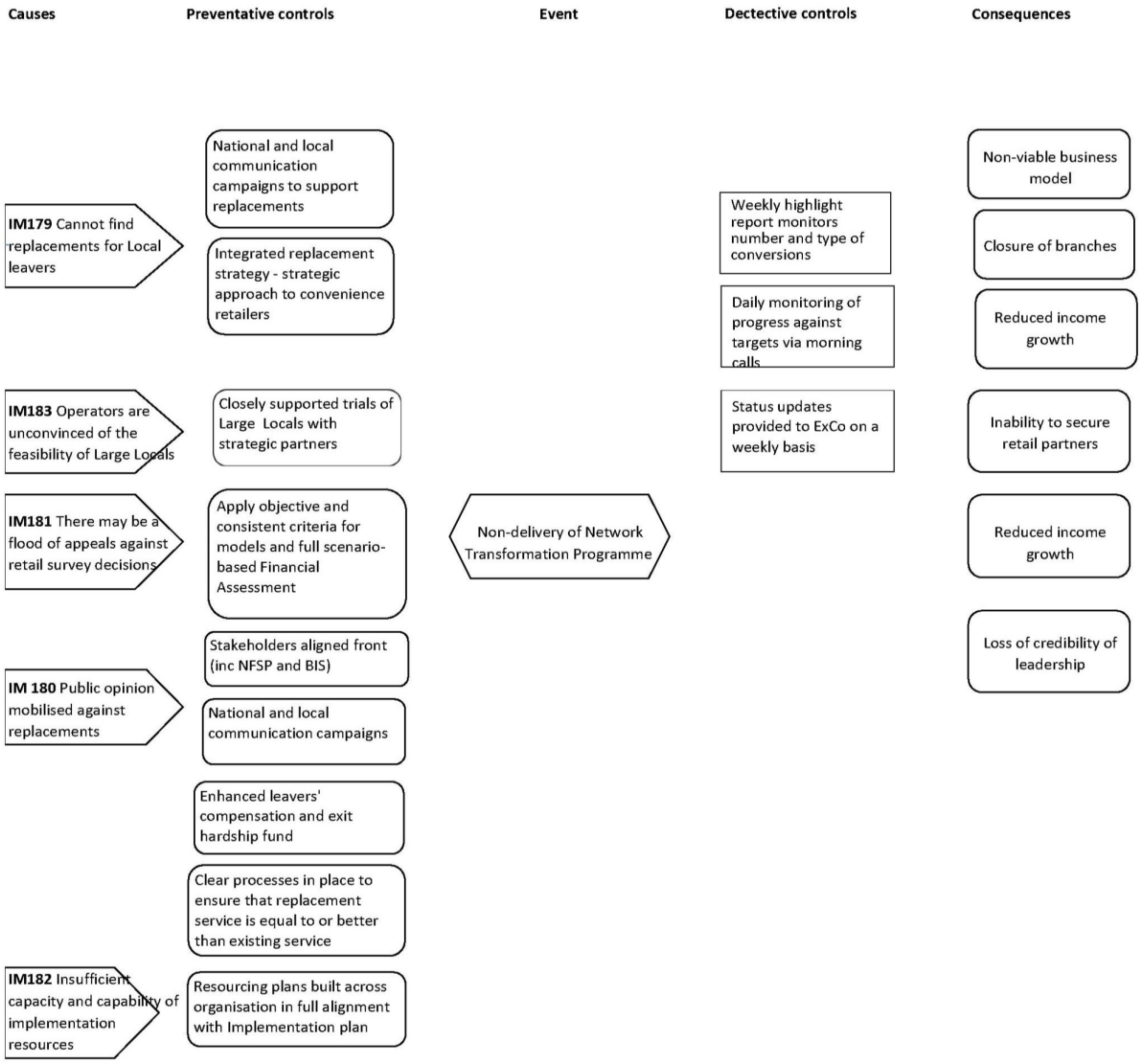
PEOPLE CAPABILITY BOW TIE: PAPER ONE APPENDIX 2

Red highlight = Work in Progress Activity



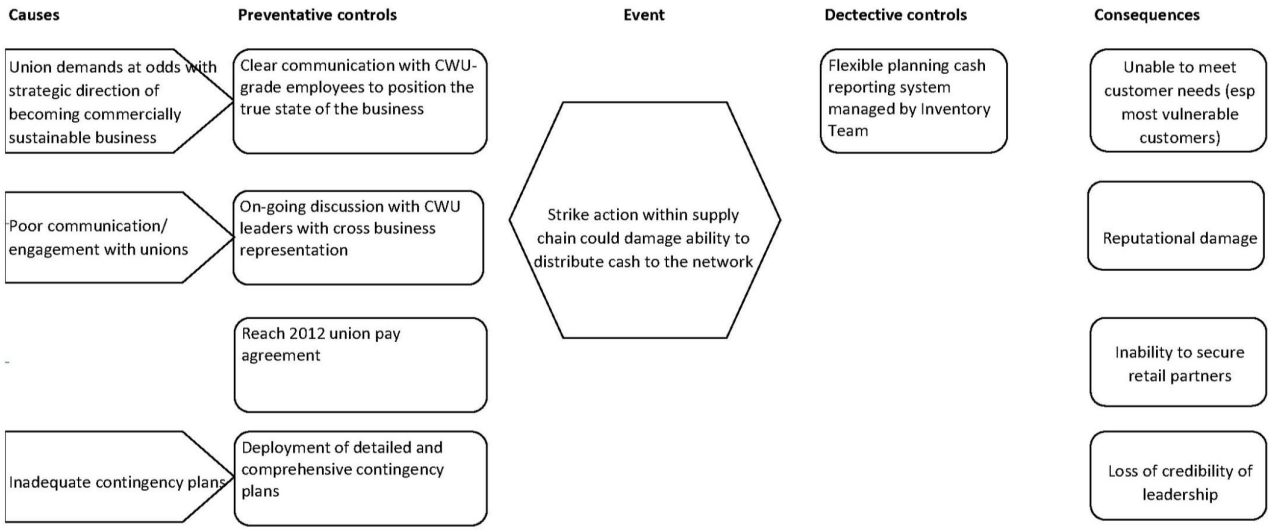
POL00333330

NETWORK TRANSFORMATION BOW TIE : PAPER ONE APPENDIX 3



POL00333330

STRIKE ACTION BOW TIE : PAPER ONE APPENDIX 4



POL00333330

DATA SECURITY BOW TIE : PAPER ONE APPENDIX 5

NOTES

(1) Supplier data identification exercise delayed due to resource constraints

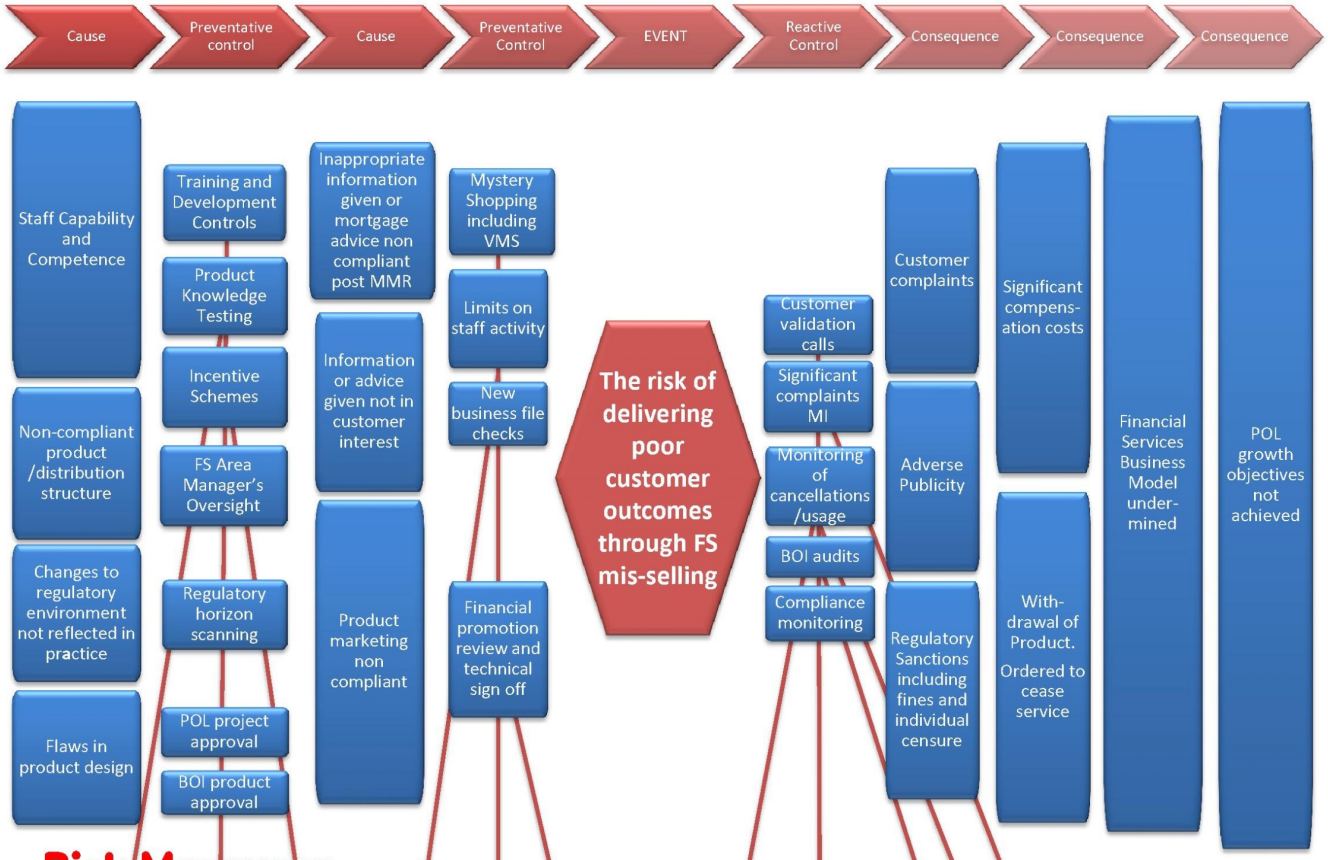
(2) Audit action on improvement of Access rights review and approval - outstanding due to lack of clarification of ownership on Identity and Access Management/Business Process Ownership

(3) Additional headcount requested

POL00333330

1. Top 10 Business Risks

FS MIS-SELLING BOW TIE – PAPER TWO



Risk Measures

Executive Summary-RISK (KRI)December

	Key performance indicators	This month's performance	
1	Video Recorded Mystery Shopping	56.5%	of recorded mystery shops received in the last period were rated red
2	Customer validation calls	98.60%	of post-sale customer calls made in the last period confirmed compliance requirements were met
3	Complaints process knowledge	7.10	of branch staff questioned in the last period could not explain how a customer could make a complaint
4	Staff product knowledge	6.7%	of product knowledge questions asked in the last period were answered incorrectly
5	Significant complaints	0.02%	of branch sales resulted in upheld significant complaints
6	Financial Promotions	95.5%	Of branches reviewed in the last 3 months met compliance standards in relation to advertising and promotions
7	Life & Over 50s cancellation rates	17.77%	of policies cancelled within the first 3 months
8	Savings Cancellations	0.67%	of savings products sold in-branch were cancelled by customers within the cooling-off period
9	Credit Card Usage	30.76%	of the credit cards sold in branch between three and nine months ago have never been used
10	Limits on staff activity MI	6.3%	Of branch staff questioned in the last month were unfamiliar with the limits on their in branch activity
11	Social Media monitoring of voice of customer	TBC	
12	BOI branch audits	TBC	

Control Improvement Actions

Supervision needs to ensure that the regulatory aspects of selling and advising that are trained out to Financial Specialists, Mortgage Specialists and other staff 'stick', become embedded and are not lost over time.

For those incentive schemes that are agreed the business need to ensure that local governance is in place to ensure regular review of the effectiveness of the schemes in driving the right behaviours.

POL00333330

Financial Services

Mis-Selling Risk Deep Dive

20th January 2014

POL00333330

Managing FS Mis-Selling Risk

Post Office, together with the Bank of Ireland (UK) ("BoI"), has a coordinated, 3 lines of defence approach to managing our conduct risk, which is focused on helping to prevent our customers from buying products that do not meet their needs.

	BoI	Post Office
1st Line	Product Teams (BoI and 3rd part product providers) Capability Development Managers	Product Teams FS Risk Sales Strategy Marketing & PR Teams
2nd Line	Risk & Compliance Financial Promotions	Corporate Risk & Compliance
3rd Line	Audit	Audit

Customers can buy our products in branch, online, via contact centres or by mail, depending on the product(s) they want. Each channel involves different risks for mis-selling.

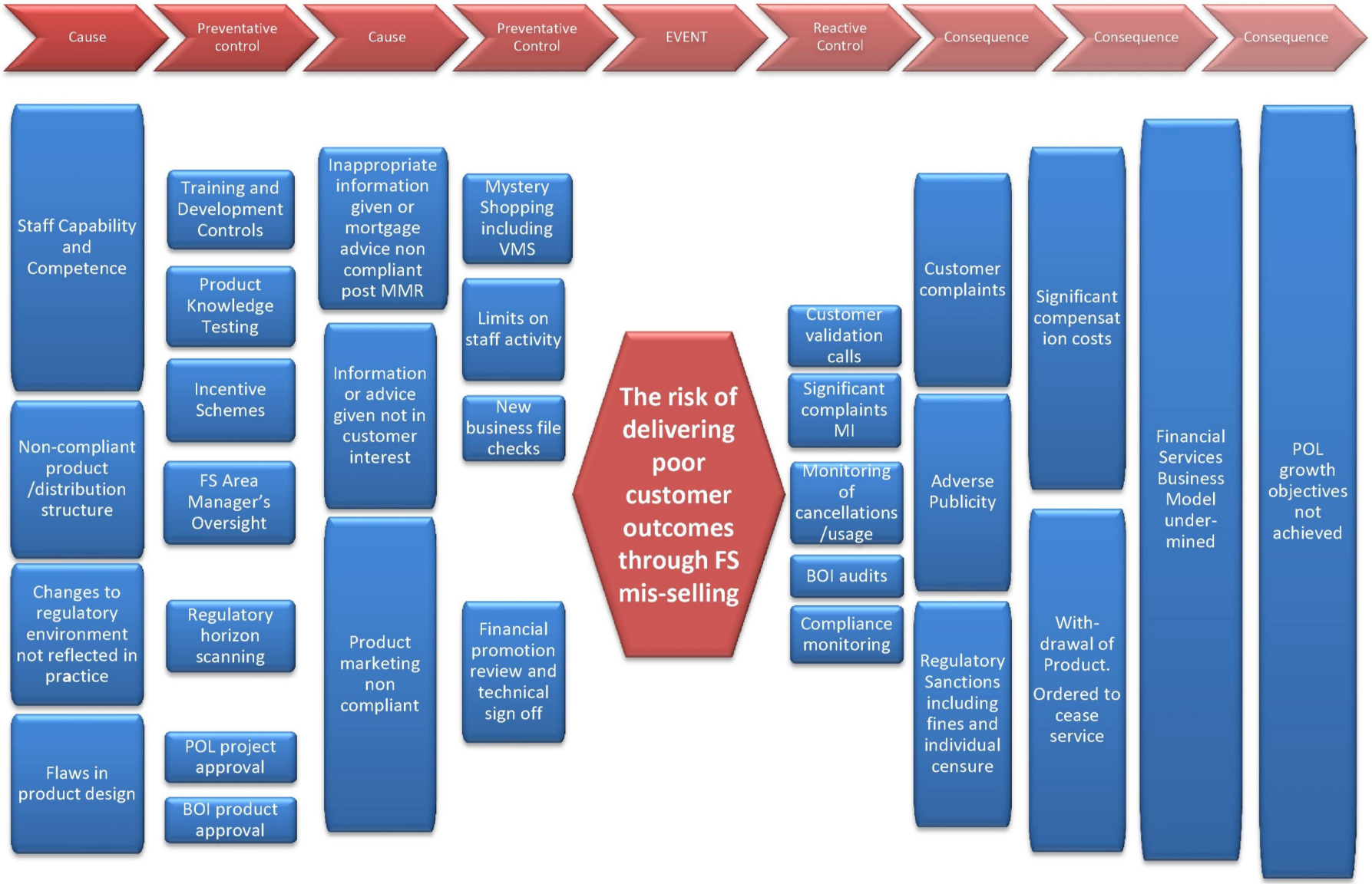
POL00333330

Key challenges today

1. Financial Specialists: training, deployment and supervision
2. MMR requirements: training and supervision of Mortgage Specialists
3. FS sales in agency: ensuring compliance and effective monitoring
4. Incentive schemes: development and deployment across channels
5. Financial promotions: maintaining compliant marketing and PR across all media including new media channels (e.g., Twitter)
6. Pace of change: ensuring we have the capacity & capability to train, deploy and monitor new products/services

POL00333330

FS mis-selling Risk "Bow-Tie"



POL00333330

FS mis-selling risk monitoring summary

Executive Summary-RISK (KRI)December

	Key performance indicators	This month's performance	
1	Video Recorded Mystery Shopping	56.5%	of recorded mystery shops received in the last period were rated red
2	Customer validation calls	98.60%	of post-sale customer calls made in the last period confirmed compliance requirements were met
3	Complaints process knowledge	7.10	of branch staff questioned in the last period could not explain how a customer could make a complaint
4	Staff product knowledge	6.7%	of product knowledge questions asked in the last period were answered incorrectly
5	Significant complaints	0.02%	of branch sales resulted in upheld significant complaints
6	Financial Promotions	95.5%	Of branches reviewed in the last 3 months met compliance standards in relation to advertising and promotions
7	Life & Over 50s cancellation rates	17.77%	of policies cancelled within the first 3 months
8	Savings Cancellations	0.67%	of savings products sold in-branch were cancelled by customers within the cooling-off period
9	Credit Card Usage	30.76%	of the credit cards sold in branch between three and nine months ago have never been used
10	Limits on staff activity MI	6.3%	Of branch staff questioned in the last month were unfamiliar with the limits on their in branch activity
11	Social Media monitoring of voice of customer	TBC	
12	BOI branch audits	TBC	

Control Improvement Actions

Supervision needs to ensure that the regulatory aspects of selling and advising that are trained out to Financial Specialists, Mortgage Specialists and other staff 'stick', become embedded and are not lost over time.

For those incentive schemes that are agreed the business need to ensure that local governance is in place to ensure regular review of the effectiveness of the schemes in driving the right behaviours.

POST OFFICE®

POL00333330

Risk Monitoring Outcomes

There have been no significant crystallised mis-selling risk events in the previous quarter.

The majority of mis-selling KRIs are green, life, Life and over 50s cancellation rates are flagged as 'amber' but as context the industry average cancellation rate sits at about 20% for these types of products.

Video mystery shops of Financial Specialists continue to demonstrate poor compliance scores. Every mystery shop is reviewed and Financial Specialists are given coaching and feedback from line managers. A wider response plan to improve compliance is in place, but our supervision needs to ensure that the regulatory aspects of selling and advising that are trained out to Financial Specialists, Mortgages Specialists and other staff 'stick' and become embedded and are not lost over time.

Mortgage market review - For the first time Post Office will be advising clients in the near future, there is increased advice and mis-selling risk. Compensating controls are being built into the new processes but until these controls are demonstrated to be effective there is uncertainty of outcome.

POL00333330

Risk Monitoring Outcomes (cont.)

New Incentive Schemes have been built with compliance gateways in place to ensure that the right behaviours are encouraged. However, a number of these have been held up by union objection including those for Financial Specialists. For those incentive schemes that are agreed the business needs to ensure that local governance is in place to ensure regular review of the effectiveness of the schemes in driving the right behaviours.

Rate and volume of change - Financial Services has a demanding growth agenda that will require more sales to be generated through a variety of channels. This includes a number of new projects, product developments and pilots, as well as work to enhance distribution channels and customer journeys at a time where the regulatory environment has become more demanding.

The new supervisory structure for Financial Specialists and Mortgage Specialists and oversight needs to bed in.

POL00333330

Strictly Confidential **PAPER THREE**

RISK & COMPLIANCE COMMITTEE

Risk Management Strategy

1. Purpose

The purpose of this paper is to update the Committee on:

1.1 progress against the risk plan
1.2 the Risk & Compliance team restructure and progress with directorate engagement

2. Background

The risk and compliance team is in the final stages of restructuring.

3. Risk Plan Update

At its last meeting the POL board was presented with details of Exco's view of the current top ten risks faced by the company (the so-called 6 +4 risks). Since that meeting:

- The terms of reference and membership of the Risk & Compliance Committee (RCC) has been reviewed in order to sharpen the committee's focus on practical, rather than abstract, risk matters. Expressly in-scope now is the monitoring of the top (ten) risks, the ongoing development of the groups risk culture, the assessment of significant risk events and the stewardship of the organisation's risk and policy frameworks. The committee membership now also expressly incudes the Chief Executive Officer (CEO) and it is envisaged that formal reports from the committee will now be a standing agenda item at future Exco meetings.

- The Risk & Compliance team has been working with the risk owners to produce a more detailed analysis of each of their main risks, identifying both the key causes and the mitigating controls. This work will be reviewed at the January RCC (due to be held the day before the board meeting). In addition the committee will at that meeting undertake a (thematic) 'deep dive' into the risks of poor customer outcomes arising through mis-selling of FS products, the work for which is near completion;

- The Risk & Compliance team has held a 2 day workshop to prepare the 2014/2015 risk management plan. This will be presented to the March Risk & Compliance Committee;

- Meetings have been held with each of the ExCo members to discuss possible "quick wins" which could be used to accelerate the changes necessary to embed a culture of risk management - a paper is in the process of being drafted summarising the actions identified at those meetings; and

- Internal Audit has been brought into the General Counsel area to promote the ongoing links between the second and third lines of defence.

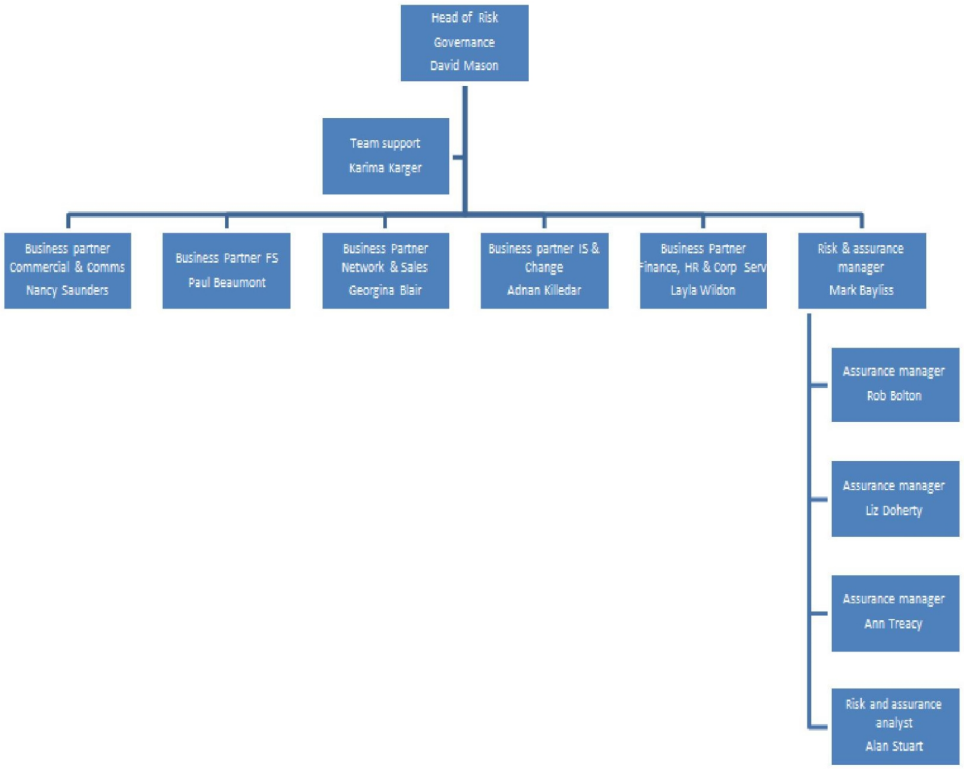
POL00333330

Strictly Confidential **PAPER THREE**

4. Risk Management Update

4.1 Restructure of the risk team

Recruitment of all current business partner roles is now finalised with two new recruits already in post. A new Business Risk and Assurance Manager joined on 3rd December. A new business partner for Information Technology & Change (IT&C) will start work on 10th February 2014. This will bring the Risk Management function up to full strength. The current Risk & Compliance team structure is shown below:



POL00333330

Strictly Confidential **PAPER THREE**

4.2 Directorate Engagement

- Good progress has been made with the risk management strategy to the end of Quarter 3;
- ExCo have met on two occasions to discuss the strategic risks to the organisation;
- The business partners have held risk workshops in six directorates and risk maps and profiles have been populated. In some directorates risk maps and profiles are in a more advanced state and good practice is being demonstrated;
- In others areas, eg Network & Sales and HR, risks have been identified and assessments are due to be carried out;
- In general, business partners meet with directorates on a monthly basis with on-going meetings to discuss risk with individual team members;
- Further workshops are planned in Communications, Strategy and the Corporate Services directorates during January and February to identify and assess their risks; and
- IT&C have identified their current risks and are updating with the help of a local co-ordinator. Assessment is continually considered in the light of the new Service Integrator and Service Desk (SISD) and organisational arrangements. A new IT&C business partner will join on 10th February and risk meetings should then be on a more frequent and continual basis.

  Further details are shown in Appendix 6.

5. Recommendations

The committee is asked to note:

5.1 The progress against the risk plan
5.2 The Risk & Compliance team re-structure and progress with directorates

Dave Mason
20th January 2014

POL00333330

PROGRESS ON THE RISK MANAGEMENT PLAN: PAPER THREE APPENDIX 6

Areas	Business Partner (BP)	Risk Map	Risk Profile	How often is the Risk Map and profile updated	How many risk meetings held with the directorate SLT and BP	Any planned meetings with the directorate SLT
Communications	Nancy			Not yet done - due 26th Jan	1	lead team meeting 26th Jan
Commercial	Nancy	yes	yes	Monthly	7 per month since September	yes - ongoing monthly 121s with lead team
ExCo	Dave/Layla	yes	yes	Quarterly	2	
Finance	Layla	Yes	Yes	Quarterly		Meeting planned w/c 13 January 2014
Financial Services	Paul	yes	yes	Monthly	4 per month approx	121s monthly with each of the leadership team
Human Resources	Layla	Yes	WIP - will change in line with strategy		Monthly with key SLT members	Quarterly with the whole Team
IT & Change	starting 10th Feb	yes	yes	bi-monthly	2	Meeting in Jan 2014
Network & Sales	Georgina	yes	WIP	Monthly	1 with whole lead team; 6 catch-ups with individuals	Next review at January SLT meeting
Operational Security	Layla	Yes	WIP	Monthly. BP attends Sec Gov. Forum	1	Meeting planned w/c 13th January 2014
Risk & Compliance	Layla					
Strategy	Layla/Nancy	WIP				w/shop booked for 20/1/14
Legal	Layla	Planned for Feb - potentially a feed to overall risk profile				
General Counsel	Layla					

POL00333330

Strictly Confidential **PAPER FOUR**

RISK AND COMPLIANCE COMMITTEE

Risk Events and Near Misses

1. Purpose

The purpose of this paper is to:

1.1 Advise the committee of the implications of internal or external incidents, events and near misses potentially impacting the risk profile of the organisation as a whole and the actions under way to remediate.

1.2 Make further recommendations to reduce the impact of similar events in the future.

1.3 Future versions will contain/show expected or actual loss for each event/near miss.

2. Internal

2.1 Outlook Mailing list misuse

On the 6th of December 2013, an employee from the Royal Mail Group issued an email to the entire Royal Mail Group and Post Office Limited in error. This mail was the catalyst for subsequent replies to the entire distribution list from multiple staff. This caused an increasing amount of pressure on the servers until the email was critically impacted with a large volume of messages queuing to be processed.

The Business Protection Team was invoked to manage the event from a Post Office perspective. Royal Mail, Post Office and its IT suppliers worked in partnership to resolve the issue, remove the email groups and restore the email service. This was completed on the same business day. Staff were then able to delete the mails and resume normal business.

The lessons learned are currently underway at the moment for preventative controls. From a corrective perspective, the email groups have been removed that will reduce the likelihood of another event.

2.2 Power supply back-up failures – Dearne House

On the 5th of December a power surge caused the Dearne House office to lose power. While the site should have a generator provision to ensure power to the site, the generator itself was impacted by the power surge and failed to initiate. This primarily impacted call centre and IT functions at the site (NBSC and the Service Desk).

The local recovery team and managers invoked contingency arrangements and calls were routed to Doxford which resulted in a queue and reduced service level.

POL00333330

The power was restored some hours later on the same day and normal business resumed.

The lessons learned is currently underway as to why the generator failed and to understand what preventative options can be deployed i.e. appropriate maintenance and Uninterrupted Power Supply (UPS). However there are on-going work streams that will reduce the impacts and likelihood of further events:

- Due to separation and transformation, Business Continuity is currently deploying the capability to recover key processes at an external facility i.e. Network Business Support Centre (NBSC). This is due for implementation by the end of February and will provide the call centre functions with recovery capability at an alternative location if Dearne House is impacted. Business Continuity is also completing an effective Business Continuity Plan for the site that will ensure the managers have a roadmap to recover critical activities during any Business Continuity event.
- The current facilities contract is under review due to separation, the Project Manager has been engaged to ensure the appropriate maintenance and testing of critical infrastructure i.e. generators and UPS.
- Power resilience will be added to the agenda of the next Business Continuity Steering Group for discussion

2.3 Swindon Power Surge

On the weekend of the 7/8th December a power surge impacted the Swindon site. Power resilience was not effective and as a result the Swindon Warehouse Control System and Galaxy ordering system were impacted on the 9th of December. As the systems were being recovered a number of issues occurred that impacted the capability for full resumption.

The Business Protection Team and Service Desk were invoked to manage the event. Contingency processes were deployed to complete critical work at Swindon. Systems were restored to a business as usual state on the 13th of December and work resumed to manage the backlog of activities and current work.

Lessons learned are currently underway to understand why the power resilience failed and what preventative options can be deployed. The following additional actions are also being completed:

- Power resilience has been added to the agenda of the next Business Continuity Steering Group for discussion.
- The current facilities contract is under review due to separation, the Project Manager has been engaged to ensure the appropriate maintenance and testing of critical infrastructure i.e. generators and UPS

POL00333330

Strictly Confidential **PAPER FOUR**

2.4 Travel Insurance

The underwriter for travel insurance products changed from Ageas to Axa from 1 January 2014. There have been a number of web site and other errors detected whilst making these changes. Business checks failed to pick up that email quotations and the Policy Summary PDFs on the website continued to refer to Ageas, this was corrected in the live environment on 2 January. There was no customer detriment as the terms and conditions of the policies remained identical and the rest of the customer journey (payment and fulfilment) remained accurate and referred to Axa.

Prices also changed on 1st January 2014. Post publication and distribution branch brochures were found to contain a price error significantly over stating the cost of one of the policy options (within Annual Multi trip cover). Over 400,000 brochures need to be withdrawn and replaced from branches as a result, at an expected cost of 55k.

The Travel team believe that POL is not liable for these costs and will be pursuing Aon/Axa for these as they were responsible for signing off the technical pricing information in the brochures, but neither firm has currently admitted liability.

Lessons learned work is being undertaken by the Regulatory Business Partner, FS, the Project Team and Digital Marketing.

2.5 Social Media misuse

Twitter -@Postofficenews posted a tweet relating to financial services that was non-compliant with the rigorous requirements set out by the Financial Conduct Authority (FCA) and had not been through the Financial Services marketing sign off process. This was picked up by the FCA who in turn made BOI aware. On this occasion the FCA didn't initiate compliance breach procedures. Communications – who run the @postofficenews twitter account were made aware of the compliance requirements, however a number of other non-compliant tweets did still get posted (but have since been taken down.)

In 2013 alone, there have been many high profile investigations of regulatory breaches that have resulted in huge fines:

Energy

- SSE were fined £10.5million for mis-selling
- Scottish Power were fined £8.5 million for misleading customers

Financial Services

- Swinton Group were fined £7.38 million for mis-selling add on Insurance
- Axa were fined £1.8 million for mis-selling ISA's

Telephony

- TimeTalk were fined £60,000 for mis-selling
- Talk Talk were fine £750,000 for making silent calls to their customers

Mail

- Royal Mail have been warned that they must improve delivery times or face fines.

Lessons learnt: There is now a work stream in place to agree use of social media

POL00333330

and appropriate controls. Until these have been agreed informed monitoring of @postoffice and @postofficenews is being carried out by Regulatory Risk and any non-compliant tweets asked to be taken down.

3. External

3.1 FCA enforcement notice and £28m fine against Lloyds Banking Group for serious sales incentives failures - Dec 2013.

This notice raises again the importance and focus the FCA has currently on incentive schemes to ensure that these drive customer focussed and compliant behaviours in sales staff. In Lloyds, case advisors continued to be rewarded for non-compliant behaviours and poor advice. The Lloyds scheme as described, by the FCA, was very aggressive in that, for example, staff could be demoted or face salary reductions if they did not hit sales targets.

Nevertheless Lloyds senior management, who would have been fully informed of the FCA's regulatory approach, were re-assured that controls were in place to mitigate risk including the use of a 'risk gateway', to ensure advisors were compliant before receiving a bonus.

The recent re-launched and other proposed POL incentive schemes for sales staff do not contain the most aggressive features of the Lloyds schemes.

3.2 Barclays Fine for record retention failure – Dec 2103

Barclays Plc has been fined $3.75 million (£2.28 million) by a U.S. regulator over its alleged decade-long failure to properly keep electronic records, emails and instant messages.

The Financial Industry Regulatory Authority said that from 2002 to April 2012, Barclays failed to preserve order data, trade confirmations, account records and other information in a format that prevented their alteration or erasure, known as "Write-Once, Read-Many".

Whilst the Post Office has data retention policies and standards they do not specifically cover emails or instant messages.

POL00333330

Strictly Confidential **PAPER FOUR**

4. Recommendations

The Committee is asked to:

4.1 Note the implications of internal or external incidents, events and near misses potentially impacting the risk profile of the organisation as a whole and the actions under way to remediate.

4.2 Agree the further recommendations below to reduce the impact of similar events in the future:

- **Lloyds Incentive Scheme**

Review the performance of the Post Office incentive schemes closely to ensure that they drive the appropriate behaviours in our customer facing staff and that we have appropriate governance to review their performance.

- **Barclays Fine**

Discuss the retention of emails and instant messages with our regulators and business partners and ensure Post Office data retention policy and practice reflects current requirements.

4.3 Note that future versions will contain/show expected or actual loss for each event/ near miss.

Dave Mason
20th January 2014

POL00333330

Strictly Confidential **PAPER FIVE**

RISK AND COMPLIANCE COMMITTEE

Assurance Activity Update

1. Purpose

The purpose of this paper is to:

1.1 Provide the Risk and Compliance Committee with an update on assurance activity that is planned, in progress, or already completed.
1.2 Ask the committee to endorse the proposed Xanadu and Mortgage Market Review assurance activity
1.3 Identify the outstanding issues and remedial actions from Rainbow

2. Assurance Activity

2.1 Rainbow

Following the Rainbow incident Deloitte were commissioned in January 2013 to provide an assessment of the Information Security operating model within Post Office and its contrast with similar organisations. Following on from the Deloitte report the actions and recommendations were incorporated into a project called Buffalo.

The Buffalo project delivered a new Information Security staffing structure and Information Security policies and procedures were reviewed and developed.

Status
The outputs from the Buffalo project have now been incorporated into business as usual, The remaining issues from the Deloitte report are:

- Information Security resources –The Group is still under resourced this is being noted as a risk
- An appropriate Information Security Risk & Compliance tool needs to be purchased and implemented.
- Data discovery exercises have been delayed due to lack of resource within the Information Security team

2.2 Governance

A review of the governance of the ExCo sub-committees has been completed and a draft report is being prepared for the General Counsel.

Status
A full update will be provided to the next Risk & Compliance Committee meeting in March 2014.

POL00333330

2.3 Mortgage Market Review

As part of a regulatory review of the mortgage market following the financial crisis the FSA/FCA has tightened the rules in a number of areas including assessment of affordability and the requirement for face to face and interactive dialogue with customers to be on an advice basis only from 26 April 2014. A major project is in place for POL/BOI to become compliant with the revised requirements. This involves a significant recruitment, training and monitoring plan for advisors alongside improved infrastructure and controls. The current project plans are graded 'green' overall and as on track to deliver the revised requirements compliantly.

Status
It has been agreed with BOI that we will jointly produce a piece of assurance work by the end of March to review whether the plans are on track and to highlight any significant risks prior to the regulatory deadline.

2.4 Xanadu

Following the fixed telephony migration an assurance review is planned which will provide an assessment of the end-to-end process for identifying and implementing the new supplier. The aim of the review is to learn lessons that can be applied to any future migration of service within the Post Office portfolio.

Status
The review is due to commence in January 2014 and terms of reference have been agreed and initial data gathering has commenced. The review will be completed in February 2014, the final report will be produced in March 2014 which will be reported to the Risk & Compliance Committee.

3. Recommendations

The committee is asked to :

- Note the update and status of assurance activity
- Endorse the proposed assurance activity to be completed for Xanadu and the Mortgage Market Review
- Consider the outstanding issues from Rainbow and any remedial actions

Dave Mason
20th January 2014

POL00333330

Strictly Confidential **PAPER SIX**

RISK & COMPLIANCE COMMITTEE

Statutory Policy Framework

1. Purpose

The purpose of this paper is to update the committee on the work planned to review the regulatory framework and to also seek approval of a number of business policies as part of the agreed policy governance process

2. Regulatory Framework

A regulatory framework was produced in February 2013 that identified regulation applicable to Post Office together with any associated policies and policy owners.

The framework now needs to be re-visited to confirm that the identified policies are still in place and have been subject to a review if required. Work is now underway to review the regulatory framework to:

- Confirm the existence of appropriate policies
- Ensure that policy owners are identified and agreed
- Ensure all policies have been subject to review as required
- Ensure all policies are captured within the new policy governance process

Progress reports will be provided to the Risk & Compliance Committee and once completed an updated regulatory framework will be produced. The current regulatory framework is attached as Appendix 7.

3. Business Policy Approvals

As part of the policy governance process all business policy documents should be submitted to the R&CC for final approval. The following business policies are therefore submitted to the January R&CC meeting for approval:

- Anti-Bribery Policy
- Acceptable Use Policy
- External Data Protection Policy
- Data Sharing Policy

It has been confirmed that the policies have been signed off at a senior level within the relevant directorate. The policies are supplied separately for information

POL00333330

Strictly Confidential **PAPER SIX**

4. Recommendations

The Risk & Compliance Committee is asked to:

- note the regulatory framework update and agree the planned activity in this area
- review and approve the policies submitted for approval and determine whether they need to be referred to ExCo for final endorsement or simply noted as approved by the R&CC

Dave Mason
20th January 2014

POL00333330

REGULATORY FRAMEWORK - PAPER SIX APPENDIX 7

	Impact	Likelihood	Risk	Policy owner	Policy	Procedure	Assurance	Commercial	Finance	Financial Services	Strategy	HR & Corporates services	Network & Sales	Communications
	Defined by the maximum level of penalty that can be imposed by the regulator in the event of a breach	Probability estimate of a breach within the current financial year	Aggregate risk calculated as the product of impact and likelihood					Marketing Sevices Digital FOoG Mails Telephony	Finance Procurement		Strategy IT & Change SPMO	HR Security Risk & Compliance Cosec Legal	Network Supply chain Property Network transformation Crown transformation Partnerships	Internal comms Press & PR Stakeholder strategy
Data Protection Act 1998	£500,000 monetary penalty, criminal offences (in certain limited circumstances), unlimited civil liabilities (for example claims from individuals who have suffered damage and distress)	High	High	HR & Corporate Services	Data protection policy Information security policy Information classification policy Mobile security policy Logical access control policy Penetration testing policy Clear desk policy 3rd party access policy Security architecture policy Security design & testing policy	SAR processes	POL Network Audit	Use of customer data for marketing purposes			Processing of customer transaction data	Use of employee data	Security of customer data in branches	
Communications Act	Up to 10% of turnover	Low	Med	Commercial	Regulated for monitoring & billing	Contract with 3rd party supplier	Twice yearly test by external party	Provision of telephony services					Sale of telephony products	
Enterprise Act 2002	Unlimited personal fines 5 year imprisonment Disqualification of directors	Low	Med	Commercial	Conflict of interest policy	Robust procurement process		Fair contracts avoiding cartels, price fixing etc	Procurement procedures Supplier tenders					
Mail Integrity Code of Practice (via MDA) Postal Services Act 2011	Breach of contract	High	Med	Commercial	Mails Distribution Agreement Mails integrity training policy Mails integrity learning policy	POL Operations manual Security operations manual Horizon On Line	POL Network Audit	Contractual obligations to Royal Mail					Acceptance and security of mail items	
Public Procurement Regulations	Ineffectiveness (contract void), unlimited financial penalty which is effective, proportionate and dissuasive, damages, restitution); other damages claims	Low	Med	Finance		Procurement teams trained in PQR Sourcing approval process in place and consistent with delegated authority levels Sourcing council in place to approve sourcing plans and allocation eSourcing RM system in use with in-built controls Standard contract terms in place for sourcing			Procurement procedures Supplier tenders					
Consumer Credit Act	Unenforceable contracts; OFT powers including civil penalties	Med	Med	Financial Services	Consumer credit licence held					Credit products			Introducing or arranging credit agreements	
FSMA (via BOI)	Unlimited fine and/or 2 years imprisonment, suspension or limitations of the approval, publication of statements regarding the misconduct. Unenforceable agreements and possible claim for loss. There is also the power to apply for injunctions and restitution orders.	Low	Med	Financial Services	BOI contract	Finprom approval procedure Regulatory Guidance Manual FSST&D scheme	BOI audit & monitoring Reg Risk Committee POL mystery shopping	Development and approval of financial promotions		Development of products and marketing	Complaints handling & monitoring		Distribution of FS products	
Corporate Manslaughter and Corporate Homicide Act 2007	Unlimited fines, remedial orders and publicity orders	Low	Med	HR & Corporate Services	H&S policies & Fleet/Buildings Management policies									
Money Laundering Regulations	-	Med	Med	HR & Corporate Services	AML policy	Suspicious activity reporting process	POL Network Audit						Money laundering in the network	
Proceeds of Crime Act 2002	Criminal offence - 14 yrs and/or unlimited fine	Med	Med	HR & Corporate Services	AML policy	Suspicious activity reporting process	POL Network Audit						Money laundering in the network	
Terrorism Acts 2000 + 2006	Criminal offence - life	Med	Med	HR & Corporate Services	AML policy	Suspicious activity reporting process	POL Network Audit						Money laundering in the network	
Electronic Communications Act	N/a	Med	Med	Strategy	Acceptable use policy Information security policy Information classification policy Mobile security policy Logical access control policy Penetration testing policy Clear desk policy 3rd party access policy Security architecture policy Security design & testing policy						Information security requirements			
PCI Data Security Standard	Fines levied by the PCI Council and/or removal from involvement with card payment schemes	Med	Med	Strategy	PCI-DSS policy Information security policy Information classification policy Mobile security policy Logical access control policy Penetration testing policy Clear desk policy 3rd party access policy Security architecture policy Security design & testing policy						Information security requirements			
Consumer Protection from Unfair Trading Regulations 2008	Court action including injunctions, undertakings and orders and publication of details thereof	Low	Low	Commercial		Manage Improvement & Change Processes Bond Pearce sign-off process for promotional materials		Design of fair products		Design of fair products				

POL00333330

Distance Selling Regulations	Court action	Medi	Low	Commercial				Direct marketing services						
UK Advertising Code/Advertising Standards Authority	Fines Reputational damage	Low	Low	Commercial		Bond Pearce sign-off process for promotional material		Development of promotional material						
Press complaints commission	Reputational damage	Low	Low	Communications										Responding to PCC
Competition Act 1998	Up to 10% of worldwide turnover; unenforceable/void contracts	Low	Low	Finance		Procurement teams trained in PCR Sourcing approval process in place and consistent with delegated authority levels Sourcing council in place to approve sourcing plans and allocation eSourcing RM system in use with in-built controls Standard contract terms in place for sourcing			Procurement procedures Supplier tenders					
Corporation Tax Acts 2009 and 2010	penalties and interest; secondary liabilities for associated companies and in limited circumstances officers of relevant companies	Low	Low	Finance	Policy is not explicitly recorded but is reflected in Senior Accounting Officer Tax certification. For 2012/13, POL will rely on RMG tax policies but will have to certify itself for SAO. Under transition arrangements, RMG will prepare returns for POL and will be asked to sign off on policies.	Procedures are recorded for Tax Senior Accounting Officer requirements. For 2012/13, POL will rely on RMG tax procedures but will have to certify for SAO. Under transition arrangements, RMG will prepare returns for POL so RMG will be asked to sign off on procedures.	SAO requirements are annual requirements, so policies and procedures will be reviewed on an annual/rolling basis. POL will need to ensure that it documents its own policies and procedures with separation and the introduction of a new accounting system.		Taxation arrangements and provisions					
Finance Act 2003	penalties and interest; secondary liabilities for associated companies and in limited circumstances officers of relevant companies	Low	Low	Finance	Policy is not explicitly recorded but is reflected in Senior Accounting Officer Tax certification. For 2012/13, POL will rely on RMG tax policies but will have to certify itself for SAO. Under transition arrangements, RMG will prepare returns for POL and will be asked to sign off on policies.	Procedures are recorded for Tax Senior Accounting Officer requirements. For 2012/13, POL will rely on RMG tax procedures but will have to certify for SAO. Under transition arrangements, RMG will prepare returns for POL so RMG will be asked to sign off on procedures.	SAO requirements are annual requirements, so policies and procedures will be reviewed on an annual/rolling basis. POL will need to ensure that it documents its own policies and procedures with separation and the introduction of a new accounting system.							
HMRC Codes of Practice 8 and 9	Criminal investigation for tax evasion (corporate and personal penalties)	Low	Low	Finance	POL aims to be categorised as "low risk" for tax accounting purposes.	Reflected in SAO certification.	POL aims to create a close working relationship with HMRC in order to be cate		Taxation arrangements and provisions					
Sale & Supply of Goods Act		Low	Low	Finance		Procurement teams trained in PCR Sourcing approval process in place and consistent with delegated authority levels Sourcing council in place to approve sourcing plans and allocation eSourcing RM system in use with in-built controls Standard contract terms in place for sourcing			Procurement procedures Supplier tenders					
Taxes Management Act	penalties and interest; secondary liabilities for associated companies and in limited circumstances officers of relevant companies	Low	Low	Finance	Policy is not explicitly recorded but is reflected in Senior Accounting Officer Tax certification. For 2012/13, POL will rely on RMG tax policies but will have to certify itself for SAO. Under transition arrangements, RMG will prepare returns for POL and will be asked to sign off on policies.	Procedures are recorded for Tax Senior Accounting Officer requirements. For 2012/13, POL will rely on RMG tax procedures but will have to certify for SAO. Under transition arrangements, RMG will prepare returns for POL so RMG will be asked to sign off on procedures.	SAO requirements are annual requirements, so policies and procedures will be reviewed on an annual/rolling basis. POL will need to ensure that it documents its own policies and procedures with separation and the introduction of a new accounting system.		Taxation arrangements and provisions					
Unfair Contract Terms (Procurement)	Unenforceable or cancelled contracts	Low	Low	Finance		Procurement teams trained in PCR Sourcing approval process in place and consistent with delegated authority levels Sourcing council in place to approve sourcing plans and allocation eSourcing RM system in use with in-built controls Standard contract terms in place for sourcing			Procurement procedures Supplier tenders					
VAT Act and SI 1995/2518	Penalties and fines for misdeclarations of VAT and in particular circumstances financial penalties for non-compliance for Senior Accounting Officer	Low	Low	Finance	Policy is not explicitly recorded but is reflected in Senior Accounting Officer Tax certification. For 2012/13, as part of RMG VAT group POL will rely on RMG tax policies and RMG will be required certify for SAO. Upon independence, POL will be required to certify itself.	VAT Procedures are recorded for Tax Senior Accounting Officer requirements. For 2012/13, as part of RMG VAT group POL will rely on RMG tax policies and RMG will be required to certify for SAO.	SAO requirements are annual requirements, so policies and procedures will be reviewed on a rolling basis. POL will need to ensure that it documents its own policies and procedures with separation and the introduction of a new accounting system.	Tax efficient contractual arrangements e.g. FS contracts	Due reporting, reconciliation & payment of VAT for income and payments					
Bribery Act 2010	Criminal Offence - Unlimited fine, Confiscation Order, Senior Officers of Company - 10 yrs and/or fine to statutory maximum.	Low	Low	HR & Corporate Services	Anti-bribery Policy			Process for partner selection, tendering	Procurement procedures Supplier tenders	Process for partner selection, tendering				
Companies Act	Fines for company officers	Low	Low	HR & Corporate Services	Company secretary in place	Delegated authority procedure			Company accounts and financial statements			Company secretary requirements		

POL00333330

Computer Misuse Act	Criminal Offence -2yrs and/or fine to statutory maximum	Low	Low	HR & Corporate Services	Information security policy Information classification policy Mobile security policy Logical access control policy Penetration testing policy Clear desk policy 3rd party access policy Security architecture policy Security design & testing policy							Information security policies and procedures		
Copyrights Designs & Patents Act Act	Injunctions, damages, undertakings and criminal penalties of up to 10 years imprisonment and unlimited fine	Low	Low	HR & Corporate Services				Brand protection						
Employee Relations regulations		Low	Low	HR & Corporate Services								Employee Relations	Employee Relations	
Employer's Liability (Compulsory Insurance) Act 1969	Reputational damage	Low	Low	HR & Corporate Services	Insurance cover	Annual renewal						Company secretary duties		
Employer's Liability (Defective Equipment) Act 1969	Civil liability	Low	Low	HR & Corporate Services	Insurance cover	Annual renewal						Employee safety		
Fraud Act 2006	Criminal Offence - 10 yrs and/or fine, Civil Liability under tort of deceit - all losses flowing from the tort	Low	Low	HR & Corporate Services					Probity of financial statements		Information security requirements			
Freedom of Information Act 2000 (FOIA)	Reputational damage; contempt of court; criminal offence - level 5 fine	Low	Low	HR & Corporate Services	Privacy Policy							Company secretary duties		
Health & Safety at Work etc Act 1974	Unlimited fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Safety Management System - safety performance monitored by ExCo Sub Comm and monthly PO Board reports	PO H&S Insp. and Audit					Employee safety		
Health and Safety (Display Screen Equipment) Regulations 1992	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	First Aid at work process and risk assessment	PO H&S Insp. and Audit						Employee safety	
Health and Safety (First-Aid) Regulations 1981	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Risk assessment process	PO H&S Insp. and Audit					Employee safety		
Health and Safety Information for Employees Regulations 1989	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Internal comms process	PO H&S Insp and Audit					Employee safety		
Limitation Act		Med	Low	HR & Corporate Services								Document retention		
Management of Health and Safety at Work Regulations 1999	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Safety Management System	PO H&S Insp. and Audit					Employee safety		
Manual Handling Operations Regulations 1992	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Risk assessment process	PO H&S Insp and Audit					Employee safety		
Occupiers' Liability Act 1984	Civil liability	Low	Low	HR & Corporate Services	Insurance cover	Annual renewal						Employee safety		
Official Secrets Act 1911 and 1989	Criminal Offence - 2 yrs and/or fine	Low	Low	HR & Corporate Services								Employee obligations		
Pensions Act	Various criminal and civil penalties for employers and individuals	Low	Low	HR & Corporate Services								Employee pension scheme		
Personal Protective Equipment at Work Regulations 1992	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Risk assessment process	PO H&S Insp and Audit					Employee safety		
Police & Justice Act 2006	Criminal Offence - 2yrs and/or fine	Low	Low	HR & Corporate Services							Information security requirements			
Private Security Industry Act 2001	Criminal Offence - 5 yrs and/or fine	Low	Low	HR & Corporate Services									CVIT	
Provision and Use of Work Equipment Regulations 1998	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Risk assessment process	PO H&S Insp and Audit					Employee safety		
Public Interest Disclosure Act 1988		Low	Low	HR & Corporate Services	Speak up (Whistleblowing policy (not approved))									
Public Records Act		Low	Low	HR & Corporate Services								Company secretary duties		
Regulation of Investigatory Powers Act 2000	Criminal Offence - 5yrs and/or fine	Low	Low	HR & Corporate Services							Information security requirements			
Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Accident reporting process	PO H&S Insp and Audit					Employee safety		
Serious Crime Act 2007	Criminal Offence - 5yrs and/or fine (and potential winding up petition)	Low	Low	HR & Corporate Services							Information security requirements			
Terms & Conditions regulations		Low	Low	HR & Corporate Services								Employee T&Cs		
Trademarks Act		Low	Low	HR & Corporate Services				Brand protection						
Transfer of undertakings (protection of employment) regulations 2006	Unfair dismissal, detriment and information and consultation awards	Low	Low	HR & Corporate Services										
Welsh Language Act	Reputational (publication of fa	Low	Low	HR & Corporate Services	Welsh Language Scheme		Customer complaints monitoring	Marketing & promotions				Recruitment of welsh speakers		
Working Time Regulations 1998	Improvement/prohibition notices	Low	Low	HR & Corporate Services								Employee safety		
Workplace (Health, Safety and Welfare) Regulations 1992	£20,000 fine and/or 2 years imprisonment	Low	Low	HR & Corporate Services	Health and Safety Policy	Risk assessment process	PO H&S Insp and Audit					Employee safety		
Construction (Design and Management) Regulations 2	£20,000 fine and/or 2 years imprisonment	Low	Low	Network & sales	Risk transfer through 3rd party contracts									
Control of Asbestos Regulations 2012	£20,000 fine and/or 2 years imprisonment	Low	Low	Network & Sales	Risk transfer through RMFM contracts								Employee safety	
Control of Substances Hazardous to Health Regulations 2002	£20,000 fine and/or 2 years imprisonment	Low	Low	Network & Sales	Risk transfer through 3rd party contracts								Employee safety	
Electricity at Work Regulations 1989	£20,000 fine and/or 2 years imprisonment	Low	Low	Network & Sales	Risk transfer through RMFM contracts								Employee safety	
Environmental Protection Act 1990 s79 causing or knowingly permitting contamination of land or water	Red diesel contimination at Chesterfield could lead to civil liability and, if enforcement notice not complied with, criminal liability	Low	Low	Network & Sales	Environmental policy									
Health Act		Low	Low	Network & Sales									Employee safety	
Highways Act 1980	Criminal Offence - Level 5 fine	Low	Low	Network & Sales		Fleet online Operatoring manuals	Monitored by Operations Compliance Team						Obstruction of highways	
Regulatory Reform (Fire Safety) Order 2005	£20,000 fine and/or 2 years imprisonment	Low	Low	Network & Sales	Risk transfer through 3rd party contracts									

POL00333330

The Road Vehicles (Construction and Use) Regulations 1996 UK domestic drivers' hours rules The road transport (working time) regulations 2005 Road traffic acts		Low	Low	Network & Sales		Fleet online Operatoring manuals	Monitored by Operations Compliance Team						POL vehicle fleet	
Carbon Reduction Commitment Energy Efficiency Scheme	Unquantified tax based on metered electricity and gas usage; payable after restructuring	Medium (depends on energy supply arrangements)	Medium	Network & Sales	Risk transfer through 3rd party contracts								POL premises - HO, network, outstations	
Environmental Permitting Regulations 2010 - causing or knowingly permitting water pollution under s12(1)(b)	Red diesel contimination at Chesterfield could lead to criminal offence	Medium ongoing risk (being assessed at present)	Medium	Network & Sales	Risk transfer through 3rd party contracts									
Equality Act 2010	Goods and services: In a successful civil court discrimination claim a Court could award an injury to feelings award (of up to £33,000) and POL may need to make alterations to premises or its practices and procedures. Employee issues:	Low	Medium	Network & Sales	Valuing diversity policy								Employee safety	

POL00333330

Post Office

Anti-Bribery Policy

The purpose of this Policy is to set standards of behaviour that minimise the risk of bribery for Post Office. The principles underpinning this Policy are the same in every country in which we operate, regardless of business sector, local customs and practices. Anyone who is employed by, or performs services for, or on behalf of, Post Office anywhere in the world in any capacity (including contractors, agents and operators, and their assistants) is bound by this Policy.

Version History

Version Number	Date	Editor	Status
0.1	16/12/13	Georgina Blair	Draft
0.2	31/12/13	Georgina Blair	Draft
0.3	08/01/14	Georgina Blair	Draft
0.4	09/01/14	Georgina Blair	Draft
1.0	16/01/14	Rob Bolton	Final

POL00333330

Version History

Date	Version	Updated by	Change summary

Document Location

The latest version of this document can be found in the Post Office SharePoint Policy Library

For Sign-off - This document has been approved by the following people:

Name	Title – Department	Date of Sign off
David Mason	Head of Risk Governance	13/01/2014
Chris Aujard	General Counsel	16/01/2014

For Information - This document will be distributed to the following people:

Name	Title – Department

This policy will be reviewed annually. Next review date January 2015.

POL00333330

Contents

POL00333330

1. Purpose

The purpose of this Policy is to set standards of behaviour that minimise the risk of bribery for Post Office. The principles underpinning this Policy are the same in every country in which we operate, regardless of business sector, local customs and practices.

Business partners are expected to act ethically and may be required to comply with this Policy in all their dealings with or for Post Office.

2. Scope and definitions

This policy applies to anyone who is employed by, or performs services for, or on behalf of, Post Office anywhere in the world in any capacity (including agents, operators and contractors).

A *bribe* is any advantage (financial or non-financial) which is promised, offered or given and is intended to induce *improper performance* (even if ineffective). *Improper performance* means carrying out a function or activity in breach of an expectation of good faith, impartiality or trust.

3. Governing principles

Post Office has a zero tolerance policy on bribery. Anybody employed by or performing services for or on behalf of Post Office

- must never promise, offer or give a bribe
- must never request or accept a bribe.

No employee will suffer demotion, penalty or other adverse consequences for refusing to pay or receive bribes or for reporting the suspicion that bribes may have been offered or accepted to Post Office, even if the refusal may result in Post Office losing business

All employees must adhere to the standards contained within Post Office's Gifts and Hospitality Approvals Procedure and the Conflicts of Interest Policy.

Any breach of this Policy, or any procedure implementing it, will be treated as a very serious matter by the company and may result in disciplinary action, including termination of employment and reporting to the appropriate authorities.

4. Business dealings and contacts

All dealings with public officials or private individuals and enterprises must be open and transparent and conducted in a proper and appropriate way. This will ensure that no bribery or corruption takes place, and will also avoid any appearance or suggestion of improper activity.

Post Office only works with business partners who have been approved as required by Post Office's risk-based due diligence processes. Such third parties must agree contractually to comply with this Policy or have an equivalent Policy in place.

Contractors must be asked to ensure that any subcontractor will comply with the principles set out in this Policy and so on throughout any supply chain.

POL00333330

Any remuneration payable to agents, operators, contractors or other business partners acting on behalf of Post Office must be appropriate for the services carried out (which is to be determined objectively as far as possible). All payments must be paid through bona fide channels, must not be made in cash and must never be made through off-shore accounts.

5. Reporting concerns

Any Post Office employee with any knowledge of or suspicions that bribery or corruption has taken place or may do so, anywhere within (or related to) Post Office, must immediately report their concerns to

- their line manager in the first instance;
- the Risk & Compliance team if the line manager cannot be contacted or cannot resolve the query; or
- the external Speak Up line in complete confidence (Tel: GRO).

All reports of suspected bribery must be passed to the Risk and Compliance team to log.

6. Roles and responsibilities

All Post Office employees are responsible for complying with this Policy and with the Gifts and Hospitality approvals procedure at Appendix A.

The Risk and Compliance team maintains a register of gifts and hospitality, and of suspected incidents of bribery, and this is reviewed regularly and an annual summary provided to the Risk and Compliance Committee and to the Post Office Board.

Any serious incidents of bribery will be escalated by the Head of Risk Governance to the Chairman of the Audit and Risk Committee.

7. Risk

Post Office has zero tolerance for bribery and all processes and procedures are designed to minimise the risk of bribery occurring. A risk assessment has been completed and the areas of the business at highest risk of bribery have been identified as Commercial, Procurement and the branch network. This policy is designed to target those areas but also applies throughout the rest of the business.

8. Contact

For further information about this policy contact the Risk and Compliance team on

GRO

POL00333330

Appendix A

Post Office Limited Gifts and Hospitality Approvals Procedure

Gifts

No gift should be offered or accepted if it is intended to induce improper behaviour. In general the giving and receiving of gifts is not permitted with the exception of low value promotional items costing under £25 each, such as pens, calendars, diaries, notepads and paperweights.

- In a situation where refusal to give or accept a gift would cause embarrassment or offence, such as when giving or receiving a gift from an overseas postal administration in an official capacity as a representative of Post Office, the gift must not appear lavish or extravagant and should not cost more than £200.
- Before giving any gift costing more than £25, written approval must be obtained from your line manager and forwarded to the Risk & Compliance team at GRO
- If you receive a gift worth more than £25 you must notify your line manager in writing, and forward the details to the Risk & Compliance team at GRO
- The Risk & Compliance team will maintain a Register of all Gifts given and received.

Hospitality

Hospitality may only be given and accepted where it has a clear and demonstrable link with a legitimate business purpose, e.g. an organised event or a meal at which business is to be discussed. In relation to offers of hospitality, numbers on both sides should be limited to those whose presence is necessary to progress the business in hand. The giving and receiving of hospitality and entertainment is subject to the following rules:

- You must obtain prior permission from your line manager before accepting or giving hospitality.
- The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £100 per person in value.
- You must send details of all hospitality offered and accepted, including details of the host business (if not Post Office Limited), the number of people attending and the businesses they represent (if Post Office Limited is the host), with details of the location of the hospitality and the cost per person, along with written approval from your line manager, to the Risk & Compliance team at GRO
- The Risk & Compliance team will maintain a Register of all Hospitality given and received.

You must beware of accepting any hospitality and entertainment which might compromise your performance of official business, or which might reasonably appear to have improperly influenced a business decision. Any attempt at entrapment, blackmail, or any suggestion that preferential treatment or divulgence of confidential information is expected in return for hospitality and entertainment, must be reported to your line manager and the Risk & Compliance team.

POL00333330

INTERNAL

Information Security and Assurance Group

IS03 - Acceptable Use Policy

Document Control

Overview

Owner:	CIO	**Enquiry point:**	Head of Information Security
Version:	1.3	**Effective from:**	
Last updated:	10th Jan 2014	**Last review date:**	10th Jan 2014
Review period:	Annually or major change		

Revision History

Version	Date	Author	Changes
1.3	10/01/2014	Moyn Uddin	Minor revision to include section 5.9.
1.2	30/05/2013	Duncan Godfrey	Updates with comments from stakeholders. Issued for ISPRC.
1.1	22/04/2013	Mark Pearce	Consistency corrections
1.0	03/04/2013	Duncan Godfrey	Updated with external review comments from Post Office Legal department. For approval.
0.4	13/02/2013	Duncan Godfrey	Minor formatting and grammar changes. Ready for approval by ISPRC.
0.3	28/12/2012	Mark Pearce	Review.
0.2	27/12/2012	Duncan Godfrey	New IS policy. Added comments from Mark Pearce and Dave King
0.1	21/12/2012	Duncan Godfrey	Reformatted from original HR release

POL00333330

1 Purpose and Statement

The purpose of this policy is to present what is acceptable use of Post Office Information Systems.

All employees of Post Office are responsible for using Post Office information resources responsibly and securely. The resources are primarily provided to support business activities.

This policy does not form part of employees' contracts and may be amended at any time.

2 Goals

The goals of this policy are to:

- Communicate what is acceptable behaviour when using Post Office Information Systems.
- Communicate the repercussions for failing to follow this policy.
- Manage the impact of the risks associated with inappropriate use of Post Office Information Systems, including: confidentiality breaches, legal claims, reputational damage, and adverse impact to the availability and/or integrity of Post Office Information Systems and loss of revenue.

3 Scope

The policy applies to all Post Office employees, agents, contractors, suppliers and consultants of Post Office.

4 Roles and Responsibilities

4.1 Information Security and Assurance Group

The Information Security and Assurance Group (ISAG) will review this policy at least annually and update accordingly to reflect changes to business objectives or risks.

4.2 Users

It is the responsibility of each user irrespective of their terms of employment or engagement to adhere to this policy.

All managers are directly responsible for implementing Post Office policies within their business areas and for their staff's adherence to them.

POL00333330

5 Policy Statement

The use of Post Office Information Systems is governed by relevant Information Security and company policies. It is the responsibility of each user to comply with these policies at all times.

5.1 General System Use

Post Office Information Systems and all the information contained within are the property of Post Office. Users are provided access to these systems for appropriate business use only.

Users may only use resources for which they have authorisation. Users may only access systems via their individual accounts and must not use another individual's colleague's account to access Post Office Information Systems.

Users are individually responsible for the resources assigned to them and are accountable to Post Office for the use of such resources.

It is the responsibility of the user to protect their passwords or any other credentials. Do not write down, display or disclose your user identity or password, or any other access code to any other individual.

Non-Post Office owned devices must not be directly connected to Post Office Information Systems (see IS16 Mobile Device Policy).

5.2 Misuse of Post Office Resources

Users must not intentionally attempt to alter the configuration of any Post Office Information System or interfere with any security control (for example anti-virus or patching updates). Users must not conduct any monitoring of Post Office Information Systems unless this has been defined as part of their role and the necessary impact assessments have been undertaken.

Users must not take any actions to anonymise their use of Post Office Information Systems.

Users shall not conduct any illegal or malicious activities using Post Office Information Systems. This includes installing any tools that could support such an activity.

5.3 Email and Instant Messaging Acceptable Use

Email and Instant Messaging (IM) are tools for conducting Post Office business and shall not be used for any other non-Post Office related business activity. All emails and IMs are archived and retained as permanent records and are subject to disclosure to outside parties including regulatory and legal authorities.

POL00333330

Users must not forward business information from business email accounts to their private non-Post Office accounts. All business emails remain the property of Post Office and must only be accessed via authorised channels.

The Email or IM facilities specifically must not be used for:

- Sending any message that others could consider indecent, offensive, threatening, insulting or derogatory
- Sending any messages that could be considered as bullying or harassing other employees, Post Office customers or any other third party;
- Sending a false and/or defamatory statement about any person or organisation;
- Sending discriminatory material;
- Distributing, disseminating or storing images, video, text or other materials that might be considered indecent, pornographic, obscene or illegal
- Creating or distributing chain letters or unsolicited advertisements (SPAM)
- Any other material that is likely to create any liability (whether criminal or civil, whether for you or us).

Any conduct listed above is likely to be seen as gross misconduct and investigated under our disciplinary procedure. Any such action will be treated very seriously and is likely to lead to the summary dismissal of the user concerned (where the user is an employee) or termination of the user's contract (where the user is not an employee).

Only Post Office approved IM facilities shall be used for business messaging..

5.4 Web Acceptable Use

Access to the web has been provide to support business activities and must primarily be used for this purpose. A certain amount of personal use is permitted (see section 5.8) but users must not:

- Access any content relating to: gambling, illegal drugs, pornography, criminal skills, hate speech or any other indecent, obscene or offensive material
- Send offensive, bullying, harassing or discriminatory material or material which is derogatory to others
- Post or otherwise transmit false or derogatory material
- Access any material which infringes copyright
- Access any material that is likely to create any liability (whether criminal or civil, whether for you or Post Office).

Any conduct listed above is likely to be seen as gross misconduct and investigated under our disciplinary procedure. Any such action will be treated very seriously and is likely to lead to the summary dismissal of the user concerned (where the user is an employee) or termination of the user's contract (where the user is not an employee).

All web access is monitored and archived; this record will be audited for compliance with this policy.

POL00333330

5.5 Use of external file storage and synchronisation services

External unauthorised file storage services (such as Dropbox, Skydrive and Googledrive, Box etc.) must not be used for storing Post Office information..

5.6 Authorised Software and Copyright Material

Users may only use the software provided to them by the Post Office IT service. No unauthorised software is permitted on Post Office Information Systems.

All users must comply with all intellectual property laws including copyright law. Any material which has a copyright must not be used on Post Office Post Office Information Systems without the correct licence. This includes: videos, audio files and any protected documents (such as restricted PDFs).

5.7 Use of social media

Post Office recognises that many of our people enjoy using social networking sites in their own time. Comments we publish on these sites may reach a surprisingly wide audience, and so we must all protect our brand and avoid doing anything that might bring the reputation of Post Office into disrepute.

Everyone must be aware that information gained about Post Office as a result of your work for the business must never be discussed or shared on social media sites.

5.8 Personal use of Post Office resources

While Post Office Information Systems are intended for business use only, our policy does allow for reasonable and occasional personal use. Any personal use must be kept to a minimum and should not interfere with an employee's business responsibilities and the resources they are using.

Personal use remains a privilege and activity conducted on Post Office Information Systems is still owned by the Post Office®. The Post Office is not responsible for the recovery of any non-business data on Post Office Information Systems and this data may be deleted at any time.

5.9 Use of Non-Post Office Equipment and Resources

Non-Post Office equipment (e.g. laptops, tablets, smartphones etc.) and or resources such as email systems (e.g. external consultancy email system, Gmail, Outlook.com (Hotmail), Yahoo Mail etc.) must not be used for Post Office business purposes, this includes forwarding Post Office information to non-Post Office email systems.

5.10 Reporting Incidents

It is the responsibility of the User to report any security incident or suspicious activity to the IT Service Desk. Advice can be sought from the ISAG.

POL00333330

5.11 Monitoring

Post Office Information Systems will be monitored and audited for compliance with this policy. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

Where we have a reasonable suspicion that Post Office Information Systems have been used improperly, in breach of the law, or if we need to assist the legal authorities or are otherwise required to do so by law, we will extend this monitoring to the content of specific electronic transactions. Only authorised individuals can undertake this activity through the Disclosure and Access to Employee Information - the "P6 process".

If an employee is concerned about personal privacy, they are advised not to use Post Office Information Systems and equipment for personal correspondence or to store personally sensitive or confidential information.

6 Exceptions

As per the standard policy process, a policy exception must be applied for by contacting the ISAG. These exceptions will be challenged and reviewed by the ISAG on an annual basis. Evidence must be retained for both the exception and the annual review.

7 Violations

Any failure to comply with this policy will be seen as a violation of the policy and may be dealt with as set out under Enforcement below.

8 Enforcement

The ISAG will regularly assess for compliance against this policy. Additionally, all Post Office people have a responsibility to report any concerns that there may have been a violation of the policy. Any violation of this policy will be investigated and is likely to be dealt with under our disciplinary procedures. In particular, any serious breach of this policy is likely to be seen as gross misconduct and could lead to the summary dismissal of the user (where the user is an employee) or termination of the user's contract (where the user is not an employee).

9 References

This document has the following references:

IS16 Mobile Device Policy

POL00333330

APPENDIX A: Glossary

	Definition
Acceptable Use	The rules on the use of Post Office Information Systems in a way which protects the reputation of Post Office and the integrity of its Information Systems and equipment.
Instant Messaging (IM)	A system for real-time electronic messaging on the Internet or over networks. The approved Instant Messaging tool in Post Office is Microsoft Office Communicator.
Post Office Information Systems	Broadly defined and includes but is not limited to: computer networks, Internet facilities, Instant Messaging systems, tablets, laptops, desktops, Personal Digital Assistants (PDA), podcasts, forums, blogs, message boards, social communication websites, newsgroups, remote access facilities and all communications through such systems.

POL00333330

EXTERNAL DATA PROTECTION POLICY

Document Control

1. Overview

Owner:	CIO	**Enquiry Point:**	Head of Information Security
Version:	2.0	**Effective From:**	01 Feb 2014
Last updated:	December 2013	**Last review date:**	02/12/2013
Review Period:	December 2014		

2. Revision History

Version	Date	Author	Amendment Details
V1	Sep 2013	Jacqueline Gazey	Initial Draft
V2	Dec 2013	Michael Hall	Minor corrections and version history added

POL00333330

Contents

POL00333330

Post Office Limited
External Data Protection Policy

1 Introduction

The processing and protection of personal information is of paramount importance to Post Office Limited (**Post Office**) in order to safeguard its reputation as one of the countries most trusted brands.

This Policy documents our approach and commitment to managing the personal information in our care, whether provided to us directly by our customers or by our business partners, in a manner compatible with our and our business partners' obligations to comply with the Data Protection Act 1998. It sets out Post Office's mandatory expectations of all those persons who have access to personal information held by Post Office on how to handle such personal information.

Adherence to this policy and associated standards is a mandatory requirement for all Post Office Representatives). Failure to comply with this policy may affect our reputation and cause our business partners not to trust our ability to manage the personal information which we hold. Compliance with this policy is essential to maintaining the confidence in our brand and our service.

2 Purpose

This Policy is aimed at all Post Office Representatives that handle personal information

The purpose of this policy is to outline the manner in which Post Office should process personal information. It sets out Post Office's expectations of its employees, sub-postmasters, agents, contractors, consultants, suppliers, partners and other contracted third parties (**Post Office Representatives**) when processing personal information entrusted to Post Office, in meeting its governing principles (set out below in section 6) relating to the use of personal information across Post Office, whether the information relates to Post Office Representatives, customers or other individuals.

3 Scope

This policy addresses all processing of personal information by Post Office Representatives whether this is information we hold directly on our customers or information we hold on behalf of our business partners.

Personal information includes all information, whether processed in electronic or structured paper form, relating to a living individual who can be identified from that information.

Processing of personal information includes the collection, use, processing, transmitting, disclosure or storage and retention of personal information. Post Office, its suppliers and contracted third must adopt procedures necessary to comply with this policy.

POL00333330

4 Status of this policy

This policy has been approved by the Post Office Board. It is managed and maintained on behalf of the Board and the Executive Team by Post Office's Privacy Team.

5 Responsibility for compliance

Post Office handles personal information on its own behalf as well as that of its business partners. The controller of the information is the party who is legally responsible for complying with the Data Protection Act 1998.

Post Office is the controller of personal information relating to individuals such as its employees, customers and prospective customers. In some cases this responsibility for customer information is shared with our Joint Venture partners who are the providers of the products and services we offer.

Where Post Office handles personal information on behalf of its business partners as a Data Processor, such as our Front Office of Government proposition, the compliance requirements will be dictated to Post Office by the appropriate Data Controller.

6 Governing principles

Personal information must always be handled by Post Office Representatives in accordance with the obligations placed on us by the Data Protection Act 1998 whether directly or through contract. This means that personal information must be:

- processed fairly and lawfully
- processed solely for the purposes it was collected for or where Post Office processes personal information on their behalf as instructed to Post Office by our business partners
- kept relevant, accurate and, where necessary, up to date
- Retained only for as long as it is necessary for the purposes it was collected, or as instructed by our business partners
- Processed in accordance with the rights granted to individuals by the Act
    - The right to access personal information about the individual
    - The right to demand the data controller cease processing likely to cause unwarranted damage or distress
    - The right to stop direct marketing
    - Rights in respect of fully automated decisions that significantly affect the individual
    - Right to claim compensation for damage (or damage or distress) caused by a failure to comply with the Data Protection Act.
- be kept secure against unauthorised or unlawful access and against accidental loss, destruction or damage by using appropriate technical and organisational measures – this includes the following:

POL00333330

- the processing of personal information should not be outsourced to agents or processors of Post Office without proper controls and contract clauses in place as established by Post Office's Privacy Manager (and the permission of the relevant business partner, where necessary).
- personal information should not be disclosed to any 3rd parties without consideration to the privacy and confidentiality commitment we have or where Post Office processes personal information on behalf of its business partners, the prior consent of that relevant business partner where required.
- Managed in accordance with Post Office's policies and procedures and where Post Office is a Data Processor, with any specific instructions provided to Post Office by the relevant Data Controller business partner.

- Not transferred overseas without additional controls being adopted to protect the rights and freedoms of the individuals as agreed with Post Office's Privacy Manager or where Post Office processes personal information on behalf of its business partners the prior consent of the relevant business partner where required

7 Accountability

Each member of the Executive Committee is responsible for compliance within their area of responsibility. Post Office's Privacy Team has responsibility for supporting the delivery of this policy and monitoring compliance with it. However, each Post Office Representative has responsibility for ensuring that they adhere to the policy.

Any Post Office Representative who considers that this policy has not been followed should raise this matter with the Privacy Team.

8 Post Office's Privacy Governance Structure

This needs to be appended once POL Exco have agreed approach

9 Further advice

Further advice may be obtained from your Post Office's Privacy Team who can be contacted by email at dataprotection GRO

10 Policy Review

This policy is scheduled for review December 2014.

POL00333330

Appendix (i) Supporting Information

Requests for access to personal information

Any individual is entitled to make a subject access request for details of personal information held about them. Where Post Office receives such requests for personal information belonging to our business partners, the process for meeting such a request sits with that business partner and Post Office will handle such requests in accordance with the instructions from our business partner.

Responsibilities of Post Office Representatives

If any Post Office Representative has access to or uses personal information about other people (e.g. customer or employee personal information) he or she must comply with this policy and the requirements set out in all other Post Office data protection standards, policies and procedures (see below).

Each Post Office Representative is responsible for ensuring that any personal information which he or she accesses or uses is kept securely and not disclosed in any way to any unauthorised third party.

Training

Where appropriate, training will be provided to Post Office Representatives on data protection issues and the handing of our business partner's personal information. Where required by our business partner to deliver specific training, such as the business partners own data protection training, Post Office will ensure that appropriate staff receive such training.

Risk assessments and audits

Periodic data protection risk assessments and audits may be carried out to assess compliance with this policy and data protection laws.

Other Post Office standards, policies and procedures relating to data protection

- Post Office Data Protection Policy (Internal)
- Code of Business Standards
- Conduct Code
- Information Security Policy & Guidance

POL00333330

Data Protection – Data Sharing Policy

Document Control

1. Overview

Owner:	CIO	Enquiry Point:	Head of Information Security
Version:	3.0	Effective From:	01 Feb 2014
Last updated:	December 2013	Last review date:	02/12/2013
Review Period:	December 2014		

2. Revision History

Version	Date	Author	Amendment Details
V1	Sep 2013	Jacqueline Gazey	Initial Draft
V2	Nov 2013	Ole Christensen	Draft with corrections
V3	Dec 2013	Michael Hall	Minor corrections and version history added

POL00333330

Contents

POL00333330

Introduction

This Policy sets out Post Office's approach to sharing information with 3rd party organisations (Recipient Organisations) and where that shared data is personal information ensures this is shared in compliance with obligations under the Data Protection Act 1998. Post Office will share information in connection with:

- The Prevention & detection of crime and prosecution of offenders
- The prevention and recovery of any loss to Post Office or one of its business partners
- National Security matters
- Anti-Money Laundering
- The protection and safety of missing or vulnerable people

Any sharing by Post Office of information to 3rd party organisations will be subject to considerations of sensitivity, confidentiality, privacy, ownership and copyright. In becoming a recipient of Post Office information, 3rd party organisations agree to process that information in line with this Policy.

Post Office information consists of personal information and business sensitive information – together referred to in this policy as "Shared Data"

Background

The Data Protection Act 1998 covers the processing of personal information and establishes rules to protect individuals in respect of the security and use of their personal information.

Post Office shares information with a number of 3rd party organisations in its endeavours to protect its business, staff, customers, other individuals and its associates.

Data Sharing

Data sharing involves the disclosure of information from one or more organisations to a third party organisation or organisations. Specifically for Post Office, data sharing can take the form of:

- a systematic disclosure of information collected by Post Office to its key contacts on a regular basis such as text blasts and reports
- Post Office and other organisations pooling information and making it available to each other for a common purpose
- exceptional, one-off disclosures of personal data by Post Office in unexpected or emergency situations
- exceptional, one-off requests by 3rd party organisations, such as solicitors, for information held by Post Office

POL00333330

Scope

This Policy covers all Post Office departments and 3rd party organisations that share Post Office personal information and business data for the purposes highlighted in section 1 below.

For the purposes of this Policy, personal information is considered to be any information that relates to a living individual who can be identified directly from the information, or from the information and other information, which is in the possession of, or is likely to come into the possession of, Post Office or the recipient organisation. This includes any expression of opinion about the individual(s) and any indication of the intentions of the Post Office or any other organisation in respect of the individual(s).

Responsibility

It is the responsibility of the signatories to this Policy to ensure it is followed in respect of the processing of shared data.

Policy.

1. Limitations on use of the data

Post Office will share information for the following purposes:

- The Prevention & detection of crime and prosecution of offenders
- The prevention, investigation and recovery of any loss to Post Office or one of its business partners
- National Security matters
- Anti-Money Laundering
- The protection and safety of missing or vulnerable people

By accepting shared data from Post Office, 3rd party recipients agree to limit their use of the shared data to these purposes only.

Where the shared data is sensitive personal information relating to:

- health information,
- racial or ethnic origin,
- religious or other similar belief,
- trade union membership,
- sexual orientation or
- offences or proceedings for an offence

the 3rd party recipient understands that the information may only be processed for:

POL00333330

- the prevention and detection of crime where such processing is in the significant public interest where such processing must necessarily be carried out without the explicit consent of the individual;
- meeting obligations placed on the organisations by way of S68 of the Serious Crime Act 2007[1];
- any legal proceedings (including prospective legal proceedings).
- The protection and safety of missing or vulnerable people where the processing is in the vital interest of the individual (or another person) in the case where consent is not available;

For shared data coming in to Post Office from one of its business partners, the same restrictions will apply.

Where a recipient of Post Office shared data wish to use the information for other purposes, Post Office's prior permission should be sought on a case-by-case basis.

2. Obligation to ensure proportionality

Post Office recognises that it is likely to be reasonable and necessary to share data in its aim to protect its staff, customers and business. Post Office will ensure that the nature of the data it shares is proportional to the above aims and will not share identifiable personal information when other methods that respect individuals' rights to privacy are viable.

3. Obligations on the parties in respect of data quality

Post Office will only share data where it is satisfied that the information is relevant to the purpose of the sharing and, to the best of our knowledge, accurate.

Where there is a requirement to keep shared data up to date on an on-going basis, the 3rd party recipient must make provisions for updates to the data on a case-by-case basis or agree its update requirements with Post Office through a bespoke data sharing arrangement

Post Office recognises that there is a requirement for information to be retained only as long as it is necessary for the purposes outlined in section 1. All recipients of Post Office shared data should have a documented retention policy outlining its intentions in respect of the archiving and destruction of this information once it has served its purpose.

4. Rights of the individual

The Data Protection Act gives rights to individuals in respect of the processing of their personal information and those key to a data sharing initiative are:

- Right of access to information;
- Right to demand an organisation cease processing personal information about them on the grounds that it will cause (unwarranted) damage or distress;

[1] Please note - S68 of the Serious Crime Act makes it an offence to further disclose information covered by this obligation.

POL00333330

- Right to object to any fully automated decisions that significantly affect the individual;
- Right to claim compensation for any damage or damage and distress caused through a breach of the Act.

In accepting personal information from Post Office, the recipient organisations accept that they will be responsible for handling any requests they receive directly from individuals in compliance with the requirements of the Data Protection Act 1998 and will adopt suitable procedures to react to individuals exercising their rights.

5. Security

Post Office takes the security of shared data very seriously. It will ensure that any information it shares with recipient organisations is transferred in a manner that protects the information, such protection being appropriate to the nature of the information and any resultant harm that could come from inappropriate disclosure, loss or destruction to that information.

Recipient organisations must ensure that shared data they receive from Post Office is adequately protected by:

- Adopting an Information Security Policy that recognises the controls required to protect this information
- Taking physical, technical and organisation security measures to protect the information
- Providing training to staff that have access to this information on the importance of keeping the information secure
- Checking the reliability of staff that are granted access to the information through formal vetting procedures appropriate to the nature of the data the staff member can see.

The recipient organisation agrees to advise Post Office immediately if, as the recipient of information, your contact information changes, your role changes or the need for sharing Post Office information stops or changes

6. Overseas Transfers

Post Office's written permission is required where Post Office shared data, disclosed to a recipient organisation that is likely to hold or allow access to the data from overseas locations. Such permission may be refused after considering the nature of the data, purpose of the processing and Post Office's obligations under the Data Protection Act 1998

7. Data Sharing using Data Protection Act 1998 exemptions

Where Post Office is approached by a 3rd, party organisation that is making a request for Post Office's Personal Information that may fall within the scope of an exemption within the Data Protection Act 1998, these requests will be considered on a case by case basis.

Post Office will apply the same considerations when using these exemptions to request other organisations for personal information.

POL00333330

8. Status of this Policy

This policy has been approved by the Post Office Executive Committee and is managed and maintained on their behalf by Post Office's Data Protection and Privacy Team.

POL00333330

Appendix (i): Obligations on Recipient Organisations

In accepting shared data from Post Office, the recipient organisation understands that it must:

a) Comply with its own obligations under the current and future Data Protection and Privacy legislation in respect of the processing of any personal data being disclosed or shared.

b) Only use the shared data for the purposes established in this Policy and not to use it for any other purpose without the prior written consent of Post Office.

c) Adopt adequate technical and organisational security measures to protect the shared data from unauthorised or unlawful processing and accidental loss, destruction or damage.

d) Advise Post Office immediately if, as the recipient of information, the contact information changes, recipients role changes or the need for sharing Post Office shared data stops or changes

e) Ensure the reliability of staff that have access to the shared data and agree that only those individuals that have a genuine business need to see that data will have access to it.

f) Only retain the shared data while there is a business need to process it and securely destroy the data in line with a documented retention schedule, as required by this Policy.

g) With regard to shared data that is personal information, respect the rights granted to individuals under the Data Protection Act 1998, adopting procedures to react to individuals exercising their rights in order to comply with the requirements of the Act.

h) Take appropriate steps to maintain the quality of the shared data.

i) Not transfer shared data outside the European Economic Area without Post Office's prior written permission as outlined in section 6 of this Policy.

j) The recipient of shared data understand that Post Office Limited is subject to the Freedom of Information Act 2000 and as such this Policy and information about those organisation that share data may be subject to disclosure under this Act.

POL00333330

Appendix (ii): Recipient Organisations

Post Office will share information with organisations, such as those that fall into the following categories:

- Law enforcement agencies
- Government bodies and agencies
- Public authorities
- Post Office product providers, for example the Bank of Ireland
- Post Office business Associates, for example Transport for London.
- Financial Services institutions, for example High Street Banks
- Sub-Post Masters
- Royal Mail
- Credit reference and fraud prevention agencies
- Financial Conduct Authority
- Legal advisors

POL00333330

Name of Organisation:

Nominated Signatory Name:

In accepting personal information from Post Office, the recipient organisation named above understands that it must:

a) Comply with its own obligations under the current and future Data Protection and Privacy legislation in respect of the processing of any personal data being disclosed or shared.

b) Only use the shared data for the purposes established in this Policy and not to use it for any other purpose without the prior written consent of Post Office.

c) Adopt adequate technical and organisational security measures to protect the shared data from unauthorised or unlawful processing and accidental loss, destruction or damage.

d) Advise Post Office immediately if, as the recipient of information, the contact information changes, recipients role changes or the need for sharing Post Office shared data stops or changes

e) Ensure the reliability of staff that have access to the shared data and agree that only those individuals that have a genuine business need to see that data will have access to it.

f) Only retain the shared data while there is a business need to process it and securely destroy the data in line with a documented retention schedule, as required by this Policy.

g) With regard to shared data that is personal information, respect the rights granted to individuals under the Data Protection Act 1998, adopting procedures to react to individuals exercising their rights in order to comply with the requirements of the Act.

h) Take appropriate steps to maintain the quality of the shared data.

i) Not transfer shared data outside the European Economic Area without Post Office's prior written permission as outlined in section 6 of this Policy.

j) The recipient of shared data understand that Post Office Limited is subject to the Freedom of Information Act 2000 and as such this Policy and information about those organisation that share data may be subject to disclosure under this Act

I acknowledge receipt of Post Office's Data Sharing Policy V1 and agree to process Post Office information in accordance with the standards recorded in this Policy.

Signed:

Dated:

POL00333330

Post Office Ltd – Strictly Confidential PAPER SEVEN

Risk and Compliance Committee (R&CC)		Reference: R&CC/MIN/OCT13
Date:	**Venue: POL Boardroom, 148 Old Street, London**	**Time: 0930 - 1130**
Attending:		
Lesley Sewell	Chief Information Officer	Member
Chris Day	Chief Financial Officer	Member
Alwen Lyons	Company Secretary	Member
Dave Mason	Head of Risk & Compliance	Chair
Malcolm Zack	Head of Internal Audit	Report
Piers Virik	SPMO	Report
Mark Pearce	Senior Risk Manager	Report
Sara Hollingsbee	Best Practice Procurement Manager	Report
Peter Emmanuel	Money Laundering Reporting Officer	Report
Liz Doherty	Assurance Advisor	Secretariat
Apologies:		
Susan Barton	Strategy Director	Member
Susan Crichton	HR & Corporate Services Director	Member

Agenda Item 1

Committee Minutes & Matters Arising

Discussion

The chair welcomed the Company Secretary to her first meeting as a committee member. Apologies had been received from Susan Barton and Susan Crichton.

The minutes of the last meeting had been circulated and were accepted as an accurate record by those present. The actions from the previous meeting were discussed and it was confirmed that with the exception of action 1552 all had been completed and closed.

Decisions

Minutes of the previous meeting were agreed and previous actions completed with the exception of 1552.

Actions

Ref	Action	Lead
1552 (carried forward)	Compile a comprehensive list of the key information security risks and identify which are important to be addressed and the resultant gaps. Skill gaps to be identified.	Julie George/Lesley Sewell

Agenda Item 2

Key Risks Tracking

Discussion

There had been no changes to the ExCo risk map since the last meeting other than the ATM rating risk was now identified as an issue. The ownership of the risk relating to the non-compliance with procurement rules was discussed together with the consequences of non-compliance.

The committee discussed the risk movements identified on the directorate risk map and agreed that the detail and quality of reasons being identified by risk owners required improvement to enable better understanding

How transformation board risks are presented to the committee in future was discussed but no decision was reached. This to be discussed and agreed outside of the meeting by the SPMO and the Head of Risk & Compliance

Decisions

The committee accepted the risk reports but identified there was a need to improve the quality of the narrative supporting risk movements identified in future reports.
Presentation of transformation board risks to be agreed by the SPMO & Head of Risk & Compliance

POL00333330

Post Office Ltd – Strictly Confidential PAPER SEVEN

Actions		
Ref	**Action**	**Lead**
1554	Presentation of transformation board risks to future R&CC meetings to be discussed and agreed	Dave Mason / Piers Virik

Agenda Item 3

Internal Controls

Discussion

The internal controls report was discussed and the committee asked about the process for improving those marked amber and how the effectiveness of identified controls was to be tested. It was suggested that the effectiveness of internal controls should rest initially with each director as the person accountable for activity within their directorate

It was also explained that Risk &Compliance business partners would be working with directorates to identify controls in place and suggest new controls and actions to achieve improvement were appropriate. The effectiveness of controls would be assured through examination of supporting management information and data with action plans developed to address any gaps and improvements.

Decisions

The committee agreed and endorsed the approach to internal controls monitoring

Actions		
Ref	**Action**	**Lead**
None		

Agenda Item 4

Key Issues Tracking

Discussion

The committee discussed the business issues log and it was agreed that any future key issues updates be supported by an explanatory paper and the issue owner should be invited to attend the meeting

Decisions

Future issues updates be supported by an explanatory paper and issue owners invited to attend future meetings

Actions		
Ref	**Action**	**Lead**
None		

Agenda Item 5

Business Policy & Consultation Approvals

Discussion

The committee reviewed the papers that had been submitted for approval.
Both papers were approved

- Disclosure &access to employee information policy
- Authority to requisition, procure and pay policy

Ownership of consultations and an approval process for their sign off has been agreed with the Communications Directorate. This is being documented and once completed will be communicated to product pillars.

Decisions

Disclosure & access to employee information policy approved
Authority to requisition, procure and pay policy approved

Actions		
Ref	**Action**	**Lead**
None		

Agenda Item 6

POL00333330

Post Office Ltd – Strictly Confidential PAPER SEVEN

Papers for Endorsement		
Discussion		
The committee reviewed the papers that had been submitted for endorsement prior to the meeting. The Money Laundering Reporting Officer's update informed the committee of actions taken as a result of an independent review which looked at POL's vulnerability to AML through products and cash services. The money laundering product risk assessment paper was discussed and agreed with the proviso that the MLRO re-issue the appendix and provide the committee with a roadmap of actions and timescales by email		
Decisions		
Both papers were endorsed with a recommendation that the MLRO re-issue the appendix and a roadmap of actions and timescales by email		
Actions		
Ref	**Action**	**Lead**
1555	Re-issue by email the appendix from the risk assessment paper together with a roadmap of actions and timescales for delivery	MLRO
Agenda Item 7		
Meeting Summary & AOB		
Discussion		
An updated R&CC terms of reference was submitted to members prior to the meeting. A proposal to hold monthly meetings was rejected and it was suggested that 6-8 meetings a year was more appropriate. The committee asked for a tracked change copy to be circulated and a request for further comments to be submitted via e mail.		
Decisions		
The terms of reference to be reviewed further.		
Actions		
Ref	**Action**	**Lead**
1556	A copy of tracked changes for terms of reference for R&CC to be circulated to members and further changes to be agreed by e mail	Rob Bolton

Liz Doherty
Risk & Assurance Adviser

POL00333330

Post Office Ltd – Strictly Confidential PAPER SEVEN

Action Summary and Updates			
Ref	**Action**	**Lead**	**Update**
1552	Compile a comprehensive list of the key information security risks and identify which are important to be addressed and the resultant gaps. Skill gaps to be identified	Julie George/Lesley Sewell	Action completed. Update provided via separate paper included with circulated meeting papers.
1554	Presentation of transformation board risks to future R&CC meetings to be discussed and agreed	Dave Mason / Piers Virik	Action closed. This has been discussed and transformation board risks to be captured within the business risk reporting to the R&CC going forward
1555	Re-issue by email the appendix from the risk assessment paper together with a roadmap of actions and timescales for delivery	MLRO	Action carried forward. Further work is currently being performed in this area and progressing through the investment committee is being explored.
1556	A copy of tracked changes for terms of reference for R&CC to be circulated to members and further changes to be agreed by e mail	Rob Bolton	Action closed. Copy of tracked changes version circulated as per the October meeting action however terms of reference have now been further reviewed and new version produced which will be circulated by email for approval

POL00333330

Risk & Compliance Committee **PAPER EIGHT**

The purpose of this paper is to provide the committee with an update on an action from a previous meeting in October 2013

1552	Compile a comprehensive list of the key information security risks and identify which are important to be addressed and the resultant gaps. Any skills gaps to also be identified	Julie George / Lesley Sewell

Consolidated Version

The Information Security and Assurance Group (ISAG), to meet its increasing responsibilities for Corporate Information Security and Assurance including Cyber Security and wider business support, require additional headcount. In addition to corporate responsibilities ISAG are responsible for the on-going Information Security due diligence of suppliers and partners to ensure that they protect Post Office information that is in their care. Currently the headcount is supplemented by 5 contractors (3 of which cover the main programmes of Transformation, Separation and Transition), where possible these Contractors are also utilised within BAU activities since there no other Information Security skills outside of ISAG within Post Office. Below is a summary table of the risk that ISAG permanent staffing shortfall creates, aside from the financial implication of the contractor overhead. The shortfall detailed on the next two tables equates to 6 FTE against the published organisation headcount shortfall of 4 (as referred to in the final perspective below).

Where possible Contractors will be replaced by full time employees providing a substantial saving to Post Office.

The comparison of Contractors versus Full time employees:

5 Contractors = (Average £850 per day x 22 days per month over 1 year) = £1,122,000
5 Full time Employees = (Average £110,000 per year inclusive of package) = £550,000

Savings £572,000 per year.

Description	**Information Risk Register**	**Role Required**
Information unavailability due to IT service disruption or lack of system availability	Covering 6 Risks	1.5 ISA Technical Assurance Manager
Information integrity and confidentiality exposure	Covering 9 risks	0.25 ISA Senior Risk manager and 0.5 ISA Compliance Manager
Insufficient Information Security involvement in wider internal practices, projects and programmes	covering 5 risks	0.5 ISA Senior Risk manager, 1 ISA Compliance manager and 1 ISA Technical Assurance Manager
Failure to conform to information security standards and compliance	covering 3 risks	0.25 ISA Senior Risk Manager and 1 ISA Compliance Manager

POL00333330

More Detailed Version			
Consolidated Risk Category	**Areas of Risk – Cause and Concern**	**ISAG Response**	**Staffing Shortfall**
Information unavailability due to IT service disruption or lack of system availability	• Communications interference • Degradation of critical services • External misuse and abuse • Insecure external communications • Loss or unavailability of premises or IT infrastructure • Malicious software	10 Penetration Tests and Vulnerability Scans undertaken annually against a projection of 30 to cover all main third parties. Whilst we do not undertake the testing ourselves there is liaison work with our suppliers as well as scoping work to ensure risks are managed appropriately	• 1.5 FTE Technical Assurance Managers
Information integrity and confidentiality exposure	• Incorrect Application Processing • Inappropriate Information Leakage • Human Error • Internal misuse and abuse • Repudiation of user action • Social engineering • Theft or loss of media • Unauthorised logical access	10 Security Reviews of significant third-parties undertaken, but at least 20 further secondary and tertiary suppliers and smaller third parties not reviewed. Review of Post Office and third party staff on internal systems only performed for privileged accounts	• 0.25 FTE Senior Risk Manager • 0.5 FTE Compliance Manager
Insufficient Information Security involvement in wider internal practices	• Inadequate third party management • Unauthorised hardware or software • Unauthorised physical access • Inadequate change management • Inadequate security awareness training(that is performed outside of ISAG) • Inadequate security incident management	ISAG is involved as : • Design Authority in contractual wording 'inclusion of 'House Position' • Licencing reviews • Physical security initiatives • IT changes • Security incidents • Maintaining the security awareness programme however gaps in coverage are apparent	• 0.5 FTE Senior Risk Manager • 1 FTE Compliance Manager • 1 FTE Technical Assurance Manager/Security Architect
Failure to conform to Information Security standards and compliance	Non-compliance to: • ISO27001 • PCI DSS • ISAE3402 • LASSIS • Third party audit and questionnaire response	Post Office manages and undertakes the contractually obligated compliance and certification activities but it is more reactive than proactive due to the increasing size of Post Office, the diversity of the business and intrusiveness of third party approaches	• 0.25 FTE Senior Risk Manager • 1 FTE Compliance Manager

POL00333330

Gaps viewed from Risk, Compliance and Technical Assurance perspective

Description	Cause	Consequence
Management of Information Risks	There was clear direction from the Buffalo exercise, Deloitte Information Security assessment review report, Internal Audit report and the PCI DSS audit the there is a significant shortfall in the way that information risks are managed. At present the area is only resourced as an interim position to cope with these activities and 1 associated extra ISA Senior Risk Manager is defined in Target Operating Model as announced on 17th Oct. There is also the growth issue of Cyber Threats which increases risk via Post Office online/digital services	This will result in ISAG team's inability to manage the new Target Operating Model defined information risk activities as they current stand. The Deloitte report stipulated "Senior Management do not have a comprehensive view on the information security risk environment" and to "plan what actions the organisation must take to reduce risk and enable Post Office to manage and monitor the threats they face effectively and proactively". The consequence of failure to attend to risks will invoke contractual and compliance penalties and sanctions
Third Parties Information Security governance	There was clear direction from the Buffalo exercise, Deloitte IS report and more importantly for on-going certification; the PCI DSS audit the there is a shortfall in the way that major third-parties are managed for assurance of their security response. Currently, there are 12 suppliers in this category, but significant others remain outside. Additionally, we need to further explore the second tier suppliers as well as complete the security review scheduled. At present the area is under resourced to cope with these activities and 1 associated extra Compliance Manager as defined Target Operating Model as announced on 17th Oct	This will result in ISAG team's inability to manage the new Target Operating Model defined compliance activities as they current stand. Furthermore both the new versions of both ISO27001:2013 and PCI DSS v3 both stipulate more requirements around the governance of third parties. The consequence of failure to attend to compliance will invoke contractual and compliance penalties and sanctions.
Information Security Technical Assurance	There was clear direction from the Buffalo exercise, Deloitte IS report and the PCI DSS audit the there is a shortfall in the way that information security technical assurance is maintained. At present the area is under resourced to cope with these activities and 2 associated extra Technical Assurance Managers as defined Target Operating Model as announced on 17th Oct	This will result in ISAG team's inability to manage the new Target Operating Model defined technical assurance activities as they current stand. Currently the management and review of vulnerability assessments, penetration testing, project technical involvement, as well as the security incident management response is under-resourced. The consequence of failure to attend to technical assurance will invoke contractual and compliance penalties and sanctions

POL00333330

Post Office Ltd
Risk & Compliance Committee
20 January 2014

Location:

Boardroom, 148 Old Street, London, England, EC1V 9HQ, United Kingdom

ATTENDANCE LIST

ATTENDEES	SIGNATURE
Alwen, Lyons	
Aujard, Chris	
Chris, Day	
Martin, Edwards	
Paula, Vennells	