POL00206524

Risk & Compliance Committee Meeting
Room 501, 148 Old Street, London, EC1V 9HQ
21st July 2014, 14.00 – 16.00

Committee Members
Chris Aujard (Chair)
Paula Vennells
Alwen Lyons
Fay Healey (attending for Neil Hayward)
Colin Stuart (attending for Chris Day)

To Attend
David Mason
Martin George
Jonathan Hill
Ian Kennedy
Paul Beaumont
Liz Doherty
Malcolm Zack (Observer)
Simon Evans (PwC Observer)

Apologies:
Chris Day
Neil Hayward

	Agenda Item	Purpose	Timings	Papers	Owner
1.	**Risk Management Culture** i) Head of Risk Report - Risk Framework Progress - Risk Events and Near Misses - Emerging Risk - Assurance Activity	**Receive report and agree any recommendations**	14.00 – 14.30 30 minutes	**Paper One (and appendix)**	David Mason
2.	**Top Business Risks** i) Deep Dive Session – Growth **a.** Financial Services **b.** Commercial	**Perform deep dive session**	14.30 – 15.00 30 minutes	**Question & Answer session**	Jonathan Hill Martin George
3.	**Assessment** i) Network Transformation Risk Mapping	**Review presentation and determine any follow up actions**	15.00 – 15.20 20 minutes	**Presentation**	Ian Kennedy
4.	**Stewardship / Framework** i) Deloitte Report ii) BCM decision iii) Policy Approvals	**Receive report and agree recommendations**	15.20 – 15.50 30 minutes	**Paper Two** **Paper Three** **No policies to be approved**	Chris Aujard David Mason N/A
5.	**Committee minutes & matters arising** i) Agree meeting minutes of 29th May 2014 ii) Matters arising from 29th May 2014	**Agree minutes and review action updates**	15.50 – 15.55 5 minutes	**Paper Four**	All
6.	**Meeting A.O.B** i) Interim R&CC Meeting Proposal ii) Attendance	**Capture and review AOB items**	15.55 – 16.00 5 minutes	**Paper Five**	All

POL00206524

Confidential **PAPER ONE**

RISK AND COMPLIANCE COMMITTEE

Head of Risk Report

1. Purpose

The purpose of this paper is to:

- provide the committee with the Head of Risk report that contains the following sections:
    - risk framework update,
    - risk events and near misses,
    - emerging risks, and
    - assurance activity.
- identify recommendations for action by the committee.

2. Recommendations

The committee is asked to:

- Receive and agree the Head of Risk report; and
- Action the recommendations made within the report.

David Mason
21 July 2014

POL00206524

Risk Framework Update

3. Approach

The Risk Framework is outlined in the risk strategy. It is designed to fit Post Office's specific needs and to support the Post Office overall strategy.

It is based on Institute of Risk Management recommendations and has been validated against international standards (ISO 31000, 31010). As elements are developed they are being reviewed with business subject matter experts.

4. Status

The current state is shown on page four of this section. The major achievements since the last meeting have been the development of a formal risk communications plan and the review and update of the Post Office risk policy.

We have revised the approach to developing the remaining risk framework elements to focus on usability and flexibility and have moved to a parallel build and deploy approach in order to:

- move at pace by developing a broader range of material in a shorter time,
- accelerate delivery by enabling a faster release and review cycle, thus
- satisfy increasing demand from the business.

The revised approach will be supported by the strategic assurance programme and enable timely integration of its outputs.

5. Significant Activity

The strategic risk profiles have been reviewed and updated after observations made during their review by ExCo.

The Kelly report on the Co-Operative Bank failure was used as the basis for a structured ExCo discussion on risk and risk governance at Post Office with a follow up discussion at the Board meeting of 16 July.

6. Resources

Due to the secondment of one member of the risk team to the Business Transformation team and the resignation and long term sickness of another, the front line risk business partner capacity is currently understaffed by forty per cent. Interim staff will be in place and recruitment to fill the permanent vacancy is under way.

POL00206524

7. Communication Plan

A communication plan has been developed, as part of the risk framework, to raise awareness of the benefits of risk management and to help deliver the risk strategy as follows:

- Key stakeholders and appropriate delivery mechanisms have been identified;
- Target groups include the Board and sub-committees, senior leadership team (SLT), business unit leadership teams, partners, project and programme management, first line risk managers, staff in specialist functions and other support staff;
- Key themes include; the roles and responsibilities of the particular group and the expectations in managing risk, the three lines of defence model and what it means, the role of the Risk Team in supporting the first line managers and the governance process which supports the framework;
- A training needs analysis is being developed to identify those who may require further risk management training in order to develop their skills in identifying, assessing and evaluating risks;
- A Risk Management intranet page is being developed to support the plan; and
- The Director of Communications is preparing a risk management communication for the SLT and business.

The next steps are to confirm target dates for the activities and to develop tailored materials to be delivered to each stakeholder group.

8. Recommendation

The committee is asked to note the progress made in building the Post Office risk framework.

POL00206524

Risk Framework Status

Risk Architecture

Complete	In progress	Planned
Governance Committees & ToR Risk reporting (internal) Assurance arrangements	Risk communication plan Risk intranet presence	Risk portfolio management

Risk Strategy

Complete	In progress	Planned
Strategy document Risk policy Review Risk priorities	Risk appetite Risk assessment techniques	Risk tolerance and capacity External reporting requirements Internal Control Framework Risk embedded in planning process

Risk Management Process

Risk Protocols

Complete	In progress	Planned
Risk acceptance Risk events Emerging risks Strategic risk register Risk maturity measurement tool	Risk identification Risk assessment and response Risk MI tool Change programme risk management and assurance Business unit risk register guidance Risk vocabulary / taxonomy	Risk training programme Internal control guidance Internal control register Operational risk register integration Programme risk register integration Risk portfolio management tool Risk and risk event escalation

POL00206524

Risk Events and Near Misses

9. New events and near misses since the last meeting

Internal Events

9.1 Travel Insurance June 2014.

Issue: Customers have purchased single trip travel insurance in-branch which either:

- provides insufficient cover for their destination of travel, or
- covers a geographical area outside their destination of travel.

The issue was highlighted when a claim was rejected due to incorrect area of cover and a complaint was made.

An investigation into the scale of the issue and the root cause has been undertaken by Financial Services (FS). A sample of cases over a 5 month period found an average of 27 cases a month with incorrect cover. Over a two year period, an estimated 2,808 policies, out of 1.1 million, may have been sold incorrectly. The root cause is that application errors made by customers or counter staff are not rejected by the Horizon system. This does not occur in telephone or web sales as these systems have fail safe cross checks in place; the sale cannot proceed until the correct details are entered into the system.

Impact: A number of post office customers have either:

- travelled with inadequate insurance cover, or
- been overcharged for insurance cover they did not need.

This will involve compensation costs, possible reputational damage and it is likely that the Bank of Ireland will have to report the issue to the FCA as a regulatory breach.

Actions: A range of actions are under way and planned.

To ensure that customers are not under insured, the FS team and Aon are undertaking a daily manual reconciliation check and upgrading the customer to the correct product, at Post Office cost, where errors are discovered.

For customers that have been over charged, Post Office is working with the Bank of Ireland to agree the next steps. It is likely that this will require contacting and compensating customers and deciding how far back in time to review. The amount of overpayment in most cases is small, £15 to £20, however the reputational risk of contacting a large number of customers' needs to be managed carefully.

A preventative control can be implemented through improvements in Horizon validation checks; this requires planning and prioritisation. In the interim, additional training is being prepared for counter staff to improve the accuracy of processing.
Owner, Paul Havenhand.

POL00206524

External Events

The following external events have happened recently. We have performed initial assessments of the potential for similar events happening in the Post Office. Further reviews may be carried out, to assess the risk and updates reported to a future meeting.

9.2 Financial Conduct Authority (FCA) fines Credit Suisse International (CSI) and Yorkshire Building Society (YBS) £2.4m and £1.4m respectively for promotions failures.

Issue: The FCA has fined both CSI and YBS for failing to ensure the financial promotions for CSI's Cliquet Product were clear, fair and not misleading. The Cliquet Product was designed by CSI to provide capital protection and a guaranteed minimum return with the apparent potential for significantly more if the FTSE 100 performed consistently well. The probability of achieving only the minimum return was 40-50% and the probability of achieving the maximum return was close to 0%. Despite this CSI's and YBS's financial promotions marketed the potential maximum return on the product as a key promotional feature. The maximum return figure was given undue prominence in both CSI's product brochures which YBS approved and provided to their clients.

Impact: If a similar flaw is identified in Post Office promotional material then Post Office would suffer significant reputational damage. If Bank of Ireland were fined as the regulated entity, Post Office could also have to compensate Bank of Ireland if agreed procedures for the review and approval of promotional material had not been followed.

Action: The risk team will confirm that adequate controls are in place to ensure that financial services promotional material is appropriately reviewed and approved.
Owner, David Mason.

9.3 FCA to assess banks' legacy IT systems as outages continue.

Issue: High street banks continue to experience service disruption due to legacy IT systems, with Royal Bank of Scotland (RBS) customers unable to pay with debit cards or withdraw cash in December 2013, a year after a high profile outage which cost the lender £175m to resolve. The FCA will now join with the Prudential Regulation Authority and the Bank of England (BOE) to assess how banks manage their exposure to IT risks, how engaged boards are with improving IT resilience, and whether they have the necessary expertise to challenge executives. The regulators will report back on findings in early 2015.

Impact: A similar failure in Bank of Ireland's systems could have an adverse impact on Post Office's Financial Services' growth strategy.

Actions: This is being discussed with the Bank of Ireland Group Technology and Change Team and we are currently awaiting their response. Owner, Alan Smith.

9.4 Gas and Electricity Markets Authority impose a financial penalty of £800,000 on British Gas Trading Ltd. May 2014.

Issue: The Gas and Electricity Markets Authority has confirmed its decision to impose a financial penalty on British Gas following an investigation into the company's compliance with regulations allowing non-domestic customers to switch suppliers.

POL00206524

Impact: Post Office telecoms customers are not required to sign a contract limiting their ability to switch. However, if they pay their rental in advance to gain a discount this will not be refunded if they leave Post Office for another supplier. This could be interpreted as a constraint on switching.

Action: The Post Office Telecoms Team is aware of this issue and has revised online and in-branch publicity material to highlight the terms and conditions of the discount for advanced payment. Owner, Hugh Stacey.

10 Update on Events previously reported.

10.1 Co-Operative Society and Network Transformation (NT) plans.

Issue: Given the current financial situation of the Co-operative Group (TCG) there is a risk that they pull out of their existing branches or look to franchise them in order to raise capital.

Impact: Temporary disruption of service if TCG pulls out of existing branches as TCG is the second biggest strategic partner. There is a possible negative impact on NT's ability to find replacements for agents leaving the network if TCG enters administration.

Actions: Work has already started to understand alternative opportunities in each community in the event that TCG wishes to pull out of their existing branches.

TCG currently has a fairly low level of interest in taking on new branches. A number of other avenues are being explored to mitigate this risk including progression with independents, symbol groups, advertising and the use of Business Transfer Agents to source new leads. All of these activities are already underway and are part of our existing BAU processes. Owner, Lillian Moshe.

Update: There is a risk register entry under the Multiples workstream to manage the risk. Financial concurrence has been given to complete the actions.

POL00206524

10.2 Kelly report – failings at the Co-operative Bank.

Issue: Failures in the Co-operative bank led to the need to adopt a Capital Action Plan to address its £1.5 billion capital shortfall. The Bank Executive failed to exercise sufficiently prudent and effective management of capital and risk. The Banking Group Board failed in its oversight of the Executive. The Group Board failed in its duties as shareholder to provide effective stewardship of an important member asset. Collectively, they failed to ensure that the Co-operative Bank consistently lived up to its ethical principles. In all these things they badly let down the Group's members.

Impact: An initial assessment was carried out to establish the impact of the Co-op's failures and to learn any lessons which could be applied to the Post Office. The weaknesses and the lessons identified by the Kelly review provide valuable insights into what can go wrong where governance and risk management are not effective.
In particular, Post Office should continue to ensure:

- Leadership's focus on governance and risk management are maintained;
- Any tendency to only listen to good news and ignore the bad is avoided;
- Assertions are challenged;
- Sufficient skilled resource is in place to avoid "capability stretch" across multiple change programmes; and
- Policies and guidance, that reflect Post Office's values and sense of purpose are in place and complied with.

Update: A questionnaire was developed by the Risk Team to assess ExCo's view of where the Post Office was in comparison to the Co-op. ExCo has discussed the item at its meeting on 3rd July and considered the next steps including the response to the Board. Owner, Chris Aujard.

10.3 BOI ATM's are not exempt from Business rate tax.

Issue: Valuation Office Agency's (VOA) decision that BOI ATMs are not exempt from Business rate tax. The VOA action is backdated for up to 3 years with a potential impact on the Post Office of up to IRRELEVANT VOA is currently seeking further clarification from the Department for Business, Innovation and Skills (BIS) on their legal position. The risk remains that VOA will send out financial demand letters. These invoices would demand payment of the full backdated amount within 30 days.

Action: The event is being closely monitored by the Banking Team within Financial Services, with continued lobbying and negotiations with BIS to try and avert a tax liability. It is not possible to determine a closure date for this event at this point in time. Owner, Alan Smith.

Update: The event has been reported to the Financial Services (FS) sub-committee on 10th June. While there has been no recent direct contact with the VOA on the issue of business rates being applied to external ATMs, engagement with BIS is on-going. BIS is continuing discussions with the VOA but no indication has been given as to the outcome and when this will be public.

POL00206524

10.4 Power Resilience Events

Issue: Two power disruptions at Dearne House and Swindon showed that power resilience plans were not effective.

Update: (1). A Business Continuity (BC) third party site has been procured and deployment of recovery capability is underway. The solution is due for full deployment and testing by the end of July 2014. (2). Project continues with Business Continuity and Power Resilience included as a required service from any nominated supplier. Business Continuity Steering Group (BCSG) reviewed Power Resilience with agreement to further review once the procurement of the enduring supplier is completed. Supplier procurement due for completion in September 2014 and power resilience review will begin thereafter. Both actions are on track to deliver by the due dates. Owner, Harry Clarke.

10.5 Change of price and product provider for travel insurance.

Issue: A number of errors occurred relating to the change of company and prices as from 1 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). Currently expected cost of correction is IRRELEVANT

Impact: The errors following the change of underwriter (from Ageas to Axa) on 1 January were reported to the January Committee. Lessons learned work was undertaken to establish the reasons for the errors in the web journey and the literature. As a result of the 'lessons learned', improvements to controls have already been implemented.

Update: The draft full report from FS, including action plans has been issued for review. Owner, Paul Havenhand.

10.6 Barclays Bank - customer data loss and Aviva - customer car insurance accident details stolen Feb 2014.

Issue: Both Aviva and Barclays have suffered theft of customer information which was later sold or offered for sale to third parties.

Impact: Controls against data leakage in the Post Office are known to be weak and would not prevent a similar theft of client data.

Actions: These incidents reinforce the need to rapidly improve Post Office data security. A programme is already under way to address data security. Specifically:

- Existing policies are due to be revised;
- Data loss prevention communications and training software have been rolled out as from April; and
- Internal Audit recommendations on user access controls are being implemented.

Update: A new Data Protection Officer started in June 2014. Work on the revision of policies has been passed to Brian Harrison, the Senior Compliance Manager who will set revised action dates.

POL00206524

11 Closed Events

11.1 Santander UK Plc. – fined £12.4m for investment advice failings.

Update: The lessons learned and actions have now been completed and the event can be closed.

11.2 Energy Supplier E.ON - fined for mis-selling.

Update: The lessons learned and actions have now been completed and the event can be closed.

11.3 ATM Cash Machines – Microsoft XP Support ends.

Update: The Product Team in Financial Services (FS) continue to monitor progress of the situation. The event can be closed.

11.4 Email disruption – Unavailability of email application March 2014.

Update: The Towers procurement contract award and assurance is to be completed by December 2014. The new arrangement will bring the contract between the Post Office and Microsoft under our ownership and control therefore negating Royal Mail intervention. This is in progress and the new provider will ensure appropriate resilience. The event can now be closed.

11.5 Big Machine – missing Destination table reference data.

Update: CapGemini (CG) have confirmed that all the actions have been completed and existing controls have been strengthened to ensure segregation of duties, appropriate access management and change control over Big Machine data. The event can now be closed.

11.6 Southport PO – incorrect disposal of customer data.

Update: An incident management report was completed and a number of recommendations were made. Some of the recommendations have been actioned eg continuing to contact the affected customers to mitigate any damage to reputation, reviewing the 'decommissioning instruction' to ensure individual roles and responsibilities are clear, communication to the Crown Network to increase awareness in identifying and destroying confidential waste. Other recommendations are being implemented eg a robust HR process for joiners, movers and leavers, a 'business owner' for Information Security Assurance Group (ISAG) incidents. The Media Relations Team and ISAG are closely monitoring the recommended actions. The event can now be closed.

POL00206524

12. Recommendations

The committee is asked to:

- Review the new events or near misses potentially impacting the risk profile of the organisation, consider the adequacy of the planned actions by Post Office and identify those requiring further monitoring;
- Note the updates on events previously reported; and
- Note the events that have been closed.

POL00206524

Emerging Risks

13. Approach

- At the last meeting in May, the committee received a paper on the emerging risks to the business and the approach adopted in identifying, managing and monitoring these risks.

- Five new risks have been added to the list. A new risk identified by the committee on State Aid and four new risks in respect of the forthcoming Welsh Language standards, the financial regulators' Fair and Effective Markets review, the effect of an increase in interest rates and the financial regulator's policy documents around culture and governance failures.

- Leading indicators are being developed for each risk to help measure the likelihood of the event happening or changes in the likelihood of the risk over time.

- The potential impacts of the risks have been updated where there have been any known changes since the last meeting.

14. Monitoring

- As we move to a monthly meeting schedule, we will report anything new at every meeting and a full update on the risks every two months.

- Awareness of the risk appetite and its application in different areas of the business will inform our decision about the amount of risk that we are willing to accept and the level of mitigation we need to apply.

POL00206524

Risk Sources	Emerging Risks	Potential impact if risk realised	Key triggers/ leading indicators	Planned Action	Risk Owner(s)
Political (New risk)	Withdrawal of state aid	The risk that the European Commission (EC) does not give clearance to our state aid proposal thus undermining funding for the Strategy 2020 plan.	EC refusal of our state aid proposal.	A draft proposal agreed with Government which complies with EC rules. The impact of accepting state aid on Post Office's restrictions policy is also under consideration.	Chris Day
Political (New risk)	The Welsh Government is due to introduce Welsh Language Standards which will replace Post Office's current Welsh Language Scheme	The standards may have a much broader impact on Post Office than our existing Welsh Language Scheme, requiring POL to provide additional services in Welsh with associated cost implications.	Publication of applicable standards; formal notification from the Welsh Language Commissioner that standards will apply to Post Office	Head of External Relations for Wales to build closer relationship with the Welsh Language Commissioner's Office to provide a better understanding of Post Office's structure, products and services. Review compliance with current Welsh Language Scheme.	Stuart Taylor
Political	The general election in 2015 results in a change of government or a change in coalition partners. (Election date 7 May 2015).	A change in government could force a change in approach to Post Office plans and strategy including, for example, network transformation as the new government may not sign up to any mandated exits	Latest Ipos-MORI opinion poll indicates: CON 31%, LAB 34%, LDEM 8%, UKIP 14%	Working to influence the 3 main party manifestos to ensure they support continuity of our strategy and business objectives.	Mark Davies
Environ-mental	Extreme weather caused by climate change leads to increased flooding which causes business disruption to branches in areas vulnerable to flooding	Flooding may result in inundation of branch premises, loss of electricity due to flooding of local substation, or staff shortages because flooding prevents travel, resulting in temporary branch closures.	NBSC stats on branch closures does not identify branch closures which have been caused by weather related flooding incidents. Bad weather was recorded as the cause of 0.56% of branch closures from Jan-Dec 2013 and 0.75% of closures from Jan – May 2014 Met Office and Environment Agency flood alerts and flood warnings	A search for past flooding incidents is completed prior to the acquisition of new Post Office owned properties. No flood risk assessment on branch premises is required from agents. When a branch reports flooding problems an assessment of the situation is made to decide whether the provision of temporary Post Office services is required. A Field Change Adviser works with the agent after the flood and some financial assistance may be	Kevin Gilliland. Harry Clarke (Property - for Post Office owned property Drew Mc Bride - Agency Network]

POL00206524

				provided.	
Risk Sources	**Emerging Risks**	**Potential impact if risk realised**	**Key triggers/ leading indicators**	**Planned Action**	**Risk Owner(s)**
Socio-cultural	A pandemic event or outbreak affecting a large proportion of the UK population. • (NB) July 14. West Africa experiencing Ebola Virus outbreak: UK GP's on alert due to possibility of infection due to people traveling to and from the region. Commonwealth Games of note due to increased travel.	Staffing plans and contingency arrangements could fail in a period of increased demand for certain services.	National Risk Register World Health Organisation (Global Tracking and threat level) BC Manager monitoring threat level and actively engaged UK Govt.	BC Manager to discuss pandemic planning with Neil Hayward and also to be discussed at next BC steering group.	Neil Hayward (TBC)
Technolo-gical	The misuse of ''Big Data'' technology by Post Office and partners	Collating information on post office customers derived from multiple sources to develop direct marketing approaches could misfire, creating significant adverse publicity.	Any new major projects with "Big Data" implications will be assessed during Gating and will be reviewed and monitored by Information Security Assurance Group (ISAG) and R&C Team for regulatory compliance.	Gating controls require risk assessments to be completed for projects. The Data Protection team within ISAG will be performing an initial investigation.	Julie George

POL00206524

Risk Sources	Emerging Risks	Potential impact if risk realised	Key triggers/ leading indicators	Planned Action	Risk Owner(s)
Legal/ Regulatory (New risk)	Fair and Effective Markets review. A joint review by the Treasury, the Bank of England and the Financial Conduct Authority will focus on those wholesale markets, both regulated and unregulated, where most of the recent concerns about misconduct have arisen: fixed-income, currency and commodity markets, including associated derivatives and benchmarks. (The review will run for 12 months from June 2014 and report by June 2015).	The potential area for the review would be FRES. FRES have confirmed that they are not in a position to manipulate the market and fix prices as they are just currency purchasers in the wholesale market. They have also confirmed they have not been contacted to take part in this review.	Invitation to take part in the review by FCA/Bank of England (BOE).	Review information updates on the FCA website.	Nick Kennett
Legal/ Regulatory (New risk)	The Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) have issued policy documents on how they propose to tackle serious failures in firms. The regulators state that where a firm presents serious risks, due to failures in culture, governance or standards, these firms will be subject to 'enhanced supervision'.	The FCA in response have re-iterated their focus on culture as a root cause of regulatory problems so this will be relevant both to how we conduct our Financial Services business as an Appointed Representative of the Bank of Ireland and when our subsidiary (Post Office Management Services) is authorised as part of project Titan.	FCA speeches outlining future regulatory approach. Post Office risk events have as their root cause poor governance or lack of consideration of customer. Conduct risk indicators reported to customer /conduct risk committee.	Risk and Compliance will be including risk culture and risk culture measures in the Post Office risk framework. Financial Services is to design and build risk culture into Post Office Management Services – project Titan.	David Mason Nick Kennett Jonathan Hill

POL00206524

Risk Sources	Emerging Risks	Potential impact if risk realised	Key triggers/ leading indicators	Planned Action	Risk Owner(s)
Legal/ Regulatory	A new Payment Services Regulator (PSR) will be fully operational in April 2015.	The role of the new PSR will be to promote effective competition, development and innovation in payment systems; and ensure payment systems are operated and developed in a way that takes account of and promotes the interests of service users. There could be increased scrutiny from this regulator or further regulatory requirements placed upon Post Office.	Review regulator website(s) eg FCA for information updates	FS are monitoring developments. After a further review with the Bank, the impacts are expected to be fairly limited as the proposed changes are in respect of the systems (eg BACS, Voco, Link) rather than customer front end processes. A watching brief will be maintained.	Nick Kennett
Legal/ Regulatory	Financial Conduct Authority (FCA) risk outlook and business plan impacts the Post Office.	There are a number of proposals that could impact on POL over the next year and beyond. - FCA thematic review-staff performance Q2 2014, - FCA thematic review-cash savings market Q4 2014, and - FCA market study-credit cards Q4 2014.	Review regulator website(s) eg FCA for information updates	The joint POL & BOI (UK) Customer and Conduct Risk Committee is monitoring developments on a monthly basis.	Nick Kennett

POL00206524

Risk Sources	Emerging Risks	Potential impact if risk realised	Key triggers/ leading indicators	Planned Action	Risk Owner(s)
Economic (New risk)	Rise in interest rates. An increase in interest rates is likely this year or early next year and forward interest rates are anticipating rate rises up to around 2.5% in 2017. Although the Governor of the Bank of England expects 2.5% to be the 'new normal' it remains possible that rates could exceed this level in the next few years.	The low interest rate environment has continued to keep debt servicing costs low and has supported indebted households and enhanced mortgage affordability. The potential downside of interest rate rises will be reduced customer budgets to purchase POL's products as well as directly impacting on mortgage sales as affordability becomes stretched. A possible upside is that higher interest rates could mean increased demand and margin on savings products.	Interest rate rises are one of the themes in the FCA's 2014 Risk Outlook document	Risk business partner will work with the business to review whether interest rate stress has been sufficiently considered in business planning. It will also be worth similarly briefing the external consultants (when appointed) to test the strategic business plans on whether sufficient consideration has been given to the impact of potential interest rate and other external economic shocks (such as a rise in inflation) in the plan assumptions.	Nick Kennett
Economic	The risk that the Post Office (POL) network is broken up as a result of a Yes vote on Scottish independence (Vote on 18 September 2014).	A separation of the network could lead to a decrease in target income and a downturn in growth.	YouGov's latest survey for the Times, shows that a large majority of Scots intend to reject independence in the referendum on September 18th. Among those who take sides 39% intend voting Yes and 61%No. THS and Ipsos MORI have recorded similar verdicts in recent weeks.	An initial high level analysis has been carried out by the Strategy Team to identify the impacts of the change.	Mike Granville and Martin Edwards

POL00206524

15. Recommendations

The committee is asked to:

- Review the new emerging risks to the business; and
- Note the updates on the emerging risks previously reported

POL00206524

Assurance Activity

16. Assurance Activity in Progress

16.1 Titan

The risk and legal teams continue to be closely involved with FS leadership and the project team in giving support, assurance and challenge where required on the efficacy of the proposals. Whilst progress has been made on a number of fronts, including agreeing a call centre partner and setting up a call centre implementation plan; the FCA application is behind schedule. This has been flagged as a key risk with the project team who have contingency arrangements in place.

The FCA Application was due to be made at the end of June. Prior to submission, further work needs to be undertaken to understand clearly the nature of the regulatory relationship between Bank of Ireland, Post Office Management Services (POMS) and Thistle Solutions (an FCA authorised firm that is offering compliance support), as well as providing more detail of the business model, risks and controls. The FCA application will be reviewed from a regulatory/legal perspective by Beachcrofts prior to submission as an assurance measure. Formal discussions with The Bank of Ireland related to Titan are expected to take place this month. It will be crucial to manage these carefully in the context of a number of other negotiations that are taking place. These relate to wider commercial agreements with Financial Services and our strategic plans (including Project Eagle).

A key risk remains the reliance on contractors to design and implement large parts of the project. Group functions (Risk and Legal) will continue to support and challenge the project where required through membership of the Titan Steering Committee and oversight of the work streams. In addition, following the submission of the FCA application in advance of any 'go live' decision, it is proposed that we will contract with external expertise to provide independent risk assurance on POMS state of preparedness prior to go live.

16.2 Rainbow

Following the Deloitte report the actions and recommendations were incorporated into a project called Buffalo. All issues from the Buffalo Project have now been resolved and:

- The Information Security governance risk & compliance tool is being implemented and the project is expected to be completed by the end of October;

- A new Data Protection Officer started on 2nd June and interviews are in progress to appoint to the remaining post; and

- The Information Security & Assurance Group have commenced the corporate wide, business impact assessment, to identify information / data assets and accountable owners within the Post Office. The original timescale of completing the initial high level assessment by June has been delayed to mid - July due to difficulties getting

POL00206524

time in director's diaries. The detailed BIA is due to be completed by the end of August.

16.3 Xanadu

The business partner responsible for the Xanadu report has resigned and is on long term sick leave. The Risk Team have had initial discussions on the recommendations from the final report with Change Management and Procurement to establish the current position. Further meetings have been arranged to identify further action required, ownership and timescales. Any actions will be co-ordinated with the strategic assurance programme.

17. Completed Assurance Activity

17.1 Mortgage Market Review

The post implementation review has now been completed and a final report has been produced and is attached with the papers. The conclusions of the review were that, with the exception of the area of Training & Development, the MMR requirements are in place and rated green. See below:

Requirements	Rating
1 Regulatory Guidance Manual and suitability guidelines including sales manual	Green
2. Fit and Proper/professional qualifications requirements	Green
3.Training materials and accreditation process	Green
4.T&D arrangements, supervision arrangements and contingency arrangements agreed	Amber
5.New Business File Checking	Green
6.Mortgage Brain and Virtual Office systems	Green
7.Suitability letters/ Execution only procedures and associated documentation e.g. IDD, KFI	Green
8.Complaints handling processes	Green
9.MMR Governance	Green

While the T&D scheme itself is 'compliant' this area was rated amber as a result of a number of known and agreed exceptions to supervisory spans of control. These exceptions were agreed as necessary to cover the first three months of mortgage advice, while the advisers were completing their initial period of close supervision..

The actions and timescales from the review have been agreed with owners prior to the final report being issued to stakeholders. All actions are scheduled to be completed by end of August.

POL00206524

.

18. Planned Assurance Activity

18.1 Strategic Programme Assurance

At the request of ExCo the strategic programme risk assurance requirements have been reviewed and identified. This includes the selection of an external strategic risk partner to accelerate Post Office change and risk management capability in the following areas:

- Change is managed in a consistent manner, using well understood tools, and reported on using a common language;
- The current dependency on external contractors is reduced, where appropriate;
- Multiple, complex programmes are delivered as an integrated whole, in a timely manner, without exposing Post Office to undue or unidentified risks;
- The ExCo (and board) receives appropriate assurance, either from internal or from third party sources or both, that the transformational risks when combined with the inherent business risks are within our overall risk appetite; and
- Robust governance procedures are in place such that future significant initiatives are authorised in full knowledge of their incremental impact on Post Office's overall risk profile.

A shortlist of three suppliers: PwC, KPMG and Grant Thornton was identified on the basis of previous work performed in similar areas and for similar organisations. Each was given a briefing on the requirement and the opportunity to ask clarifying questions.

Formal presentations were made to the key internal stakeholders including the, General Counsel, Head of Risk, Head of Internal Audit and Head of Change Management by each of the shortlisted suppliers. PwC was selected on the basis of the quality of their proposal, extensive prior experience and relative value for money. Initial diagnostic work has started.

19. Recommendations

The committee is asked to note the update on assurance activity

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

Programme	Mortgage Market Review	**To**	Jeremy Law, John Wilcock, Jonathan Hill, Paul Beswick, Martin Brown, Dave Mason
Date	20 June 2014	**From**	Paul Beaumont, Liz Doherty

EXECUTIVE SUMMARY

The Financial Conduct Authority (FCA) Mortgage Market Review (MMR) reforms set out the case for reforming the mortgage market to ensure it is sustainable and works better for consumers. The majority of the MMR regulations came into effect on 26 April 2014. The Post Office launched an advised 'MMR compliant' mortgage service through Crown branches on 3 February 2014. The scope of this review was to assess whether the following MMR regulatory requirements were in place for mortgage advice in POL branches (see scope and background to review in Appendix).

Overall the conclusion is that the requirements are in place although the T&D requirements have been rated amber (as at April 2014). While the T&D scheme itself is 'compliant' this area was rated amber as a result of a number of known and agreed exceptions to supervisory spans of control. These exceptions were agreed as necessary to cover the first three months of mortgage advice, while the advisers were completing their initial period of close supervision. This does however place strain on the supervisory structure which is being relieved through the temporary supervision arrangements.

Requirement in scope	Rating
1 Regulatory Guidance Manual and suitability guidelines including sales manual	Green
2. Fit and Proper/professional qualifications requirements	Green
3.Training materials and accreditation process	Green
4.T&D arrangements, supervision arrangements and contingency arrangements agreed	Amber
5.New Business File Checking	Green
6.Mortgage Brain and Virtual Office systems	Green
7.Suitability letters/ Execution only procedures and associated documentation eg IDD, KFI	Green
8.Complaints handling processes	Green
9.MMR Governance	Green

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

Green-In place

Amber-In place but further work required to ensure continued compliance

Red- Not in place

1. Regulatory Guidance Manual (RGM) and Suitability Guidelines including Sales Manual

RGM

Bank of Ireland (Bank) provided to POL, updated regulatory guidance to take into account the revised advice process ahead of 'go live'. This was aligned to the processes that had been designed prior to launch and these were agreed by POL as deployable.

Suitability Guidance

A mortgage advice procedure and standards manual is in place. This explains in a compliant and user friendly way Post Office's advice standards. We note that this document has a review date of January 2015 but we would expect this document to be regularly updated in line with expected changes in the business.

2. 'Fit and Proper'

When the regulator drafted the MMR review it was expected that Mortgage Advisors would be 'Approved Persons' in a similar way to other individuals in the Financial Services market offering financial advice i.e as per the CF30 Customer Function). The FCA requirements cover 'Honesty and Integrity', 'Financial Soundness' and 'Competence and Capability'. This requirement has not, so far, been implemented by the regulator and it is still unclear whether this will happen at a future date

Bank and POL agreed that we would apply to Mortgage Advisors, standards similar to those required by the FCA for Approved Persons. It also agreed to apply these requirements to their supervisors (FSAMs) and senior supervisors (RMs). This reflects the clear importance of these new advice giving roles and also acts as a preventative control if FCA were to extend the Approved Persons regime to Mortgage Advisors at a future date. After the announcement that additional checks were to be carried out it prompted withdrawal of some applications.

POL required all candidates to fill out and submit to HR an additional form covering FCA (Form A) requirements. HR engaged with a reference checking firm 'Backcheck' to check the additional information - such as reference checking and directorships- that HR's routine vetting processes do not currently cover for staff of this category. HR also included this requirement in contracts of employment.

Status

Approximately one third of all applications had areas that required further consideration in respect of Fit and Proper. This includes details disclosed (or undisclosed) in relation to career history, inconsistencies in employer dates, CCJs, Bankruptcy and references from previous employers. So far there has been no evidence of criminal record activity uncovered by the checking process.

POL00206524

A master database is retained within the HR Centre which records status and results for all the Fit & Proper tests for Mortgage Specialists, Area Sales Managers and Regional Sales Managers. A review of the database confirms that the requirements of the Fit & Proper Test have been carried out and results entered on the database.

Issues or inconsistencies that arise in the process have been discussed at a weekly committee meeting with appropriate POL Senior Line Management, HR, Risk Management and Bank representation. An audit trail of the decisions made on applications and their rationale are recorded on a master database held by the HR manager. So far, a decision has been made not to approve one individual.

Recommendations

1. Based on the history of precedent that has built up from the Fit and Proper cases reviewed so far, draft procedures should be drawn up by HR on how to review 'Fit and Proper' cases in the BAU environment and incorporated into the POL vetting policy. Exception cases to the adopted procedures should be flagged to the Controlling Supervisor and Bank/POL Compliance for review.
2. Consideration to be given as to how we consider 'Fit and Properness' on an on-going basis following initial acceptance. This could, for example, be on the basis of an annual self-assessment questionnaire that can be subject to random checking by HR.

2a Professional Qualifications

The FCA requirements are that Mortgage Advisors are required to have appropriate professional qualifications (generally either CeMap or CF1 and CF6). For those that do not have the required qualification the FCA rules give advisors 30 months from when they begin the activity of mortgage advise to obtain the qualification. T&D has strongly supported internal candidates providing access to intensive exam support training and Webinars. As at 07/04/2014 there were 11 Mortgage Specialists 'live' under enhanced supervision required to pass the CF6 qualification, out of an active population of c80.

The RGM and T&D scheme both reflect the revised regulatory requirements. The RGM also requires those individuals supervising Mortgage Specialists to have the appropriate regulatory qualifications prior to supervising and this has been enforced.

The current Mortgage Specialist population is made up of external entrants and Financial Specialists that have applied to become Mortgage Specialists. All external candidates were required to have the requisite qualifications prior to entry and these were checked by HR. Internal candidates are required by the T&D scheme to obtain the CF1 qualification prior to entering training and the CF6 qualification within a year of entering enhanced supervision. Tracking spread sheets are in place for T&D to review the qualification status of all MSs. However, there does appear to be a gap with respect to recording examination passes formally. These confirmations and certificates are not currently copied to T&D and the individual T&D files.

Recommendation

1. Record of exam passes (copy certificates) for both external and internal candidates to be copied into local T&D files.

POL00206524

3. Training Materials and Accreditation Process

We have reviewed a selection of the training materials provided to attendees as well as the accreditation process. The training process appears comprehensive and includes system training as well as advice training and was given to both internal and external candidates

Accreditation at the end of training for mortgage specialists requires the training team to assess candidates' product knowledge, 2 case studies, a process test and 2 role plays covering both stages of the sales process. FSAMs undertake the same core training with additional work on supervision; they are required to pass the product knowledge and process test as well as 3 case studies and 3 observations prior to accreditation.

An accreditation sheet is signed off by the training team outlining whether the candidate has met, exceeded or passed with development needs. . Development needs are outlined in the accreditation form. The accreditation form outlining development needs are passed on to the Mortgage Specialist, the supervisor and the T&D team.

4.Training and Development (T&D) Arrangements and Supervision.

Robust T&D arrangements are key to ensuring that post accreditation, a professional and compliant advice process continues to be delivered to customers. The T&D scheme has been significantly updated to take into account the Mortgage Advice requirements and the interaction with the Bank Quality Checking Unit. All the stages of the scheme have been updated to reflect this covering;-

- Initial Training and Accreditation
- Close/Enhanced Supervision
- On-going Supervision
- Supervisor Training and Accreditation
- Supervisor Close Supervision
- Supervisory Guidance
- Dealing with Incidents of non-competence
- Continuous Personal and Professional Development
- Exceptions/Absences and Contingency Arrangements

In the first three months of Mortgage Advice, compliance with the T&D requirements are expected to be stretched reflecting the new arrangements and that all Mortgage Advisors are under either close or enhanced supervision from day one and that there are also a large number of supervisors (FSAMs) under close supervision (currently 12 out of 33) and all of our 3 Regional Managers (senior supervisors) are relatively new.

The senior supervisor span of control (RM to FSAM) has been maintained at below 14 which is compliant under the scheme. The required span of control for supervisors (FSAMs to Financial Specialist/ Mortgage Specialist) is not based on an absolute number, but determined under the scheme using risk rating factors (points) related to the specialism and competence level of the specialist and also whether the supervisor himself is under close or continuous supervision. A competent FSAM is permitted a supervisory point span of 20 and an FSAM under close supervision is permitted a point score of 10.

Based on the latest April data out of 33 FSAMS;

-9 competent FSAMs were exceeding the 20 point span of control limit.

POL00206524

-8 FSAMs under close supervision were breaching the 10 point supervision limit (including. one FSAM under close supervision with a supervisory span of 33 points).

As a temporary arrangement, to cover supervision gaps in the field three Capability and Development Managers from Bank and one sales trainer from Post Office was currently covering supervisory gaps in the field as a result of current vacancies.

T&D oversight

There is a significant amount of MI to inform the T&D team on the performance of the scheme and advisors. This has been able to identify poorly performing advisors and supervisors. Currently 5 FSAMS have been identified as higher risk. Based on MI received and file reviews the T&D team have also suspended two Mortgage Specialists pending re-training following concerns raised.

The T&D team undertake risk based random sampling of advice cases checked by FSAMs to assess supervisory competence. The T&D team also receive reports from the QA unit. These are key 'end quality' reports on advice requirements and these are all followed up by the T&D team with supervisors and specialists. A significant range of other data is available to the T&D team on an individual advisor basis. Some of this has recently been reformatted into a Compliance scorecard as part of the compliance gateway to the MS/FSAM incentive schemes. This includes pass rates for product knowledge tests, product cancellation rates, video mystery shopping results and significant complaints information.

Compliance with the scheme is also maintained by collecting data from supervisors and senior supervisors confirming when T&D activity (such as one to one meetings and observations) have been completed with the T&D team then updating a central excel spread sheet.

To review the quality of the T&D activity completed (such as 121s, evidence of coaching, managing people, observations and development plans) the T&D team undertake quarterly sampling of T&D files to review the quality of T&D work undertaken. Feedback is given by the T&D teams to supervisors on the quality of the T&D activity undertaken.

Recommendations

1. Consideration to be given as to the types of CPD activity that will be appropriate for Mortgage Specialists to undertake going forward. Whilst there is no compulsory requirement under the MMR rules FCA still expects firms to regularly review mortgage specialists competence to ensure they remain competent for their role, as per the rule at TC 2.1.12.
2. To re-review in the requirements of the scheme spans of control based on risk and the numbers of FSAMs and Mortgage Specialists obtaining 'continuing supervision' status. This should also take into account planned changes to the business including growth plans as well as other initiatives.
3. Compose a list of high risk mortgage specialists and FSAMs. This should be based on file review data, QA unit findings and other relevant MI (such as VMS) to review their accreditation status and on on-going fitness to operate in a regulated environment.

5.Quality Assurance (QA) Checking Unit

Quality Assurance checking was outsourced to the Bank. The independent QA unit reviews cases advised and submitted by Mortgage Advisors. These are graded:

POL00206524

Mortgage Market Review

FINAL REPORT

A Pass-*The advice provided is clearly justified and the documentation contains no errors.*
B Pass-Advice provided is justified but documentation contains minor error or inconsistency.
C Fail- It is not possible to determine whether the advice is appropriate from the information contained in the documentation.
D Fail-It is possible to determine that the advice is incorrect based on the evidence and the justification provided

E Unable to assess, documentation is incomplete.

In accordance with the T&C scheme the first 10 cases an advisor submits are 100% checked by the QA team. For MS's under close or enhanced supervision this criteria can only be relaxed if they achieve a pass rate of 80% or more on submitted cases. If this mark is achieved and provided the supervisor, the QA team and the T&D Manager all agrees then this checking rate can reduce to 50% of cases submitted.

Based on conversations with the field and the T&D team, the MI and communications arrangements between the QA team, MSs and FSAMs, appear to be generally working well. However, it is the view of T&D that the QA reports could be improved by;-

i) becoming more timely, potentially moving from monthly to bi- monthly reporting to enable a more rapid response to identifying issues (March cases were reported on 15 April)
ii) Improving the granularity of failure reporting so that T&D can understand at a deeper level the root causes of failures.

The latest (March) report from the QA unit reports a 76% pass rate (A&B grades). However, 20% of the cases not passing are Band Cs. This grading refers to cases where the reviewer believes there is missing information on the case, for example some potentially missing information on the 'key' information system. Once the missing information is provided these cases will then either be migrated to an A or B pass grade or to a D failure grade.

It is arguable whether this grade should not be denoted a 'red' fail but as an unrated transitory grade until the missing information is provided. Particularly since the vast majority of these cases are ultimately deemed 'suitable advice'. However, there are also arguments that the case should be failed because the advisor should produce all the detail required to enable a case to pass first time. As the checking process is new it will be worth reviewing whether the grading criteria work for all parties.

<u>Recommendations</u>

1. T&D team and QA unit to liaise on detail and regularity of MI pack reporting
2. Whilst out of the scope of this report, it is worth noting that POL has no oversight over the QA checking process for advice given from the POL mortgage call centre. POL should undertake further work to satisfy itself that the standard of checking for these cases is appropriate and that a consistent approach is being taken overall.

POL00206524

6.The Key, Mortgage Brain and Virtual Office Compliance

These systems alongside 'SalesForce' are the systems Mortgage Advisors use to collect and record client information at point of sale to for product search and to complete the mortgage application. These systems can be accessed in real time from Head Office by the Product Manager to review cases under construction by advisors, to help resolve mortgage queries and to help liaise with Bank regarding underwriting decisions.
The system appeared to work compliantly at Head Office and also when we reviewed this in operation in the field with a Mortgage Specialist.

The big drawback operationally is the need to use three separate systems to capture client information, to review mortgage choices and to submit the formal application to Bank. This requires a degree of duplication with the specialist having to re-key details between systems. This increases additional preparation time for mortgage advisors and is likely to contribute to an increased rate of case mistakes and inconsistencies.

Recommendation

1. Bank/POL to review scope for improvements in point of sale, customer data capture, product search and application systems. Consider whether investment should be made to systems to reduce risk and cost and to deliver an improved service to the customer in the context of the growth strategy for mortgages.

7.Suitability Letters/Execution Only procedures and associated documentation eg Initial Disclosure Document, Key Facts Information

The MMR 'Execution only' procedures have been adequately captured in the Mortgage Advice procedure and standards manual and the sales training.

At point of sale for the branch we visited, appropriate documentation was being produced such as the IDD, KFI, and Suitability Letters (with appropriate space to capture soft facts).

Recommendation

1. .Produce a combined IDD (CIDD) to cover that we provide an advised service for mortgages and a non-advised service for all other products.

8. Complaints Handling Process

The Post Office Branch Complaints process has been developed and is outlined in the process document V2 dated January 2014. The complaints handling process is working, operational and MI is produced from the complaints handling team (see example below).

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

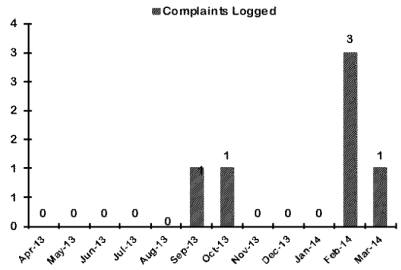
Monthly Case Reports - UK Mortgages - Society 1 PO

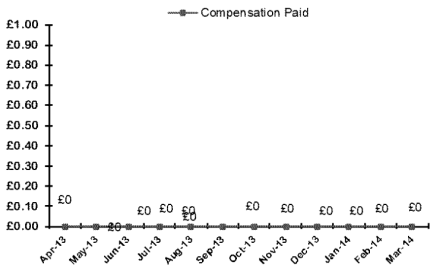
PO Mortgages Branch - March 2014

Issued By: Group Complaints MI

Historic Trends - Rank 2 - Insufficient info provided

Month	Complaints Logged	Compensation Paid
Mar-14	1	£0
Feb-14	3	£0
Jan-14	0	£0
Dec-13	0	£0
Nov-13	0	£0
Oct-13	1	£0
Sep-13	1	£0
Aug-13	0	£0
Jul-13	0	£0
Jun-13	0	£0
May-13	0	£0
Apr-13	0	£0
12Months	6	£0





Insufficient info provided - (Complaints Logged - Mar-14

PO Branch	PO Advisor	Ref	Logged Date	Complaint
337965		CRC/06017-14	07/03/2014	Borr unhappy with the advice received by Debbie in Norwich PO Branch. The mortgage offer she provided them with was not available due to the borr's being existing customer's.

The next steps are to review that all the MI flows for advised mortgage sales complaints are being reported to the advisor, supervisor, the T&D team and T&D file and to ensure that upheld complaints are fed into the Compliance gateway (for the incentive scheme). We may in the future need to provide regulated references for Mortgage Specialists and this will require us to maintain records of upheld complaints during their employment.

Recommendation.

1. T&D to work with the complaints unit to ensure that detailed information on complaints is reaching all parties including the T&D team.

MMR Governance.

As part of the MMR implementation programme a significant programme of MMR governance was evidenced. This included the MMR Steering Committee (this was the senior forum for overseeing implementation), the MMR Joint Working Group, Programme Boards as well as local delivery groups e.g. complaints.

It is also worth noting in this context that the FCA conducted a review into BOI mortgage strategy between September and December 2013 to assess the governance arrangements to ensure sufficient consideration is given to the customer. In the context of mortgage strategy governance, the FCA concluded that there were adequate governance arrangements in place.

The MMR Steering Committee remained in place post 'go live' implementation, but these arrangements have been replaced by new arrangements for business as usual. The membership and Terms of Reference for these Committees have now been agreed (see below).

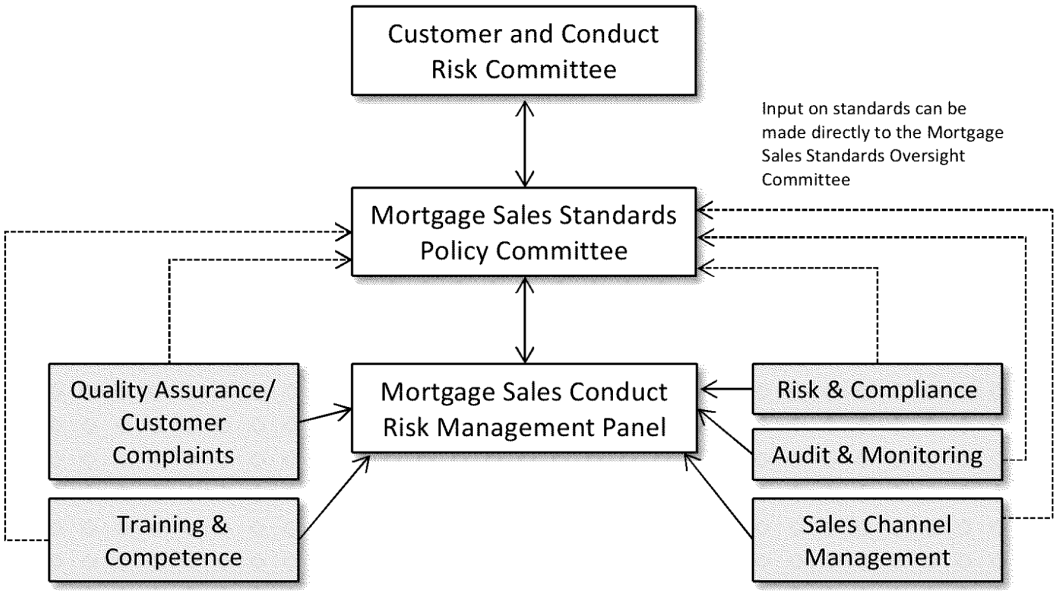
POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

Proposed Governance Structure for Bank/POL final agreement -March 2014 (version 2.0)



The Mortgage Sales Standards Policy Committee is a joint BOI/POL committee which reports into the existing Customer and Conduct Risk Committee and is responsible for the maintenance, oversight and development of mortgage related sales standards.

The Mortgage Sales Conduct Risk Management Panel is a joint BOI/POL operational forum which reports into the Mortgage Sales Standards Oversight Committee. It is responsible for monitoring and reviewing the quality of mortgage sales activity and for recommending appropriate action to mitigate and/or prevent customer detriment and to improve mortgage sales standards.

ENDS

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

Appendix 1

RISK REVIEW-TERMS OF REFERENCE

Background

The Financial Conduct Authority (FCA) Mortgage Market Review (MMR) reform set out the case for reforming the mortgage market to ensure it is sustainable and works better for consumers. The majority of the MMR changes come into effect on 26 April 2014. Those that will be most relevant for intermediaries such as the Post Office are covered in the appendix attached. A project was put in place to ensure that both POL and Bank were compliant in advance of the MMR requirements. POL went live with advised sales in branches from 3 February.

Objective

The scope of the review is to assess whether the following MMR regulatory requirements are in place for mortgage advice in POL branches.

Scope

- Regulatory Guidance Manual and suitability guidelines including sales manual
- Fit and Proper/professional qualifications requirements
- Training materials and accreditation process
- T&D arrangements, supervision arrangements and contingency arrangements agreed
- New Business File Checking
- Mortgage Brain and Virtual Office systems compliance
- Suitability letters/ Execution only procedures and associated documentation eg IDD, KFI
- Complaints handling processes
- MMR Governance
-

Outside of Scope

The prudential requirements of MMR (affordability, stress tests etc) and direct /call centre sales and advice

POL00206524

Appendix 2

MORTGAGE MARKET REVIEW (MMR) REGULATORY BACKGROUND

The FCA's MMR reform set out the case for reforming the mortgage market to ensure it is sustainable and works better for consumers. The majority of the MMR changes come into effect on 26 April 2014. Those that will be most relevant are:
For intermediaries such as the Post Office;-

- The removal of the requirement on intermediaries to assess affordability.
- The removal of the non-advised sales process.
- Most interactive sales (e.g. face to face or telephone) to be advised.
- An 'execution only' sales process for non-interactive sales (internet and postal).
- Every seller required to hold a relevant mortgage qualification.
- It will no longer be compulsory to provide customers with an Initial Disclosure Document (but firms can continue to do this if they want to). Instead, certain key messages about a firm's service must be given to customers.
- The Key Facts Illustration will not have to be given every time the firm provides the customer with information about a product that is specific to them. Instead, it will only be required where a firm recommends a product or products, where the customer asks for a KFI, or where the customer has indicated what product they want in an execution-only sale.

For lenders such as Bank of Ireland

- Lenders will be fully responsible for assessing whether the customer can afford the loan, and they will have to verify the customer's income. They can still choose to use intermediaries in this process, but lenders will remain responsible.
- Lenders will still be allowed to grant interest-only loans, but only where there is a credible strategy for repaying the capital.
- There are transitional provisions in the MMR that allow lenders to provide a new mortgage or deal to customers with existing loans who may not meet the new MMR requirements for the loan. The borrowing will not be able to exceed the amount of their current loan, unless funding is required for essential repairs. The decision on whether or not to lend in these cases will remain with the lender.

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

Appendix 3

MORTGAGE MARKET REVIEW (MMR) RECOMMENDATIONS & ACTIONS

Para	Recommended Action	Owner	Timescale	Status
2 (1)	Draft procedures to be drawn up for how to review Fit & Proper cases in BAU environment and also the handling of exception cases. Agreed procedures to be included in the Vetting Policy	Steve Holdbrook	31/07/2014	Initial draft and processes to will be ready to circulate by end of June
2 (2)	Draft a process for re-testing Fit and Properness on an on-going basis.	Paul Beaumont to take forward with BOI/HR	31/08/2014	To be discussed with HR
2A	A copy of exam pass certificates for all internal and external candidates to be copied into local T&D files.	Jayshree Patel	31/07/14	Internal exam pass certificates have been obtained (not filed). External copies are to be obtained from HR
4 (1)	Review the types of CPD activity appropriate for Mortgage Specialists to undertake going forward.	Jayshree Patel	31/07/2014	Work in progress
4 (2)	Review the span of control of the T&D scheme allowing for growth and other business initiatives.	Jayshree Patel Paul Beaumont	31/07/2014	It is understood that spans have recently been reduced. PB to confirm and review with JP
4 (3)	Compose a list of high risk mortgage specialists and FSAMs to review their fitness to operate in a regulated environment	Jayshree Patel	31/05/2014	In place for both FSs as well as MSs.
5 (1)	POL T&D and Bank QA to agree MI pack reporting	Jayshree Patel	31/07/2014	Being discussed with the Bank
5 (2)	Complete a review of the QA checking process for advice given from the POL mortgage call centre.	Paul Beaumont to review results from Bank Compliance	31/08/2014	Bank compliance plan to review by 31 July

POL00206524

PAPER ONE APPENDIX **RISK & COMPLIANCE COMMITTEE**

Mortgage Market Review

FINAL REPORT

		Review		
6	Review scope for improvements in capture and application of POS customer data by the MS and delivery of improved customer service	John Wilcock	TBC	Improvements are currently being investigated by Bank/POL, but as this involves strategic investment in IT, there is likely to be a long lead time if changes are agreed
7	Produce a combined IDD (CIDD) to inform customer of services that POL can provide	Jayshree Patel	31/07/2014	The Bank is reviewing and will be responsible for compliance sign off.
8	Confirm that Complaints data is being circulated to all parties.	Jayshree Patel	31/07/2014	In progress

POL00206524

Confidential **PAPER TWO**

POST OFFICE LTD

RISK AND COMPLIANCE COMMITTEE

Project Zebra - Horizon review by Deloitte

1. Purpose

The purpose of this paper is to:

1.1 Summarise the work undertaken by Deloitte, their approach, key findings, and their recommendations; and

1.2 Outline POL management's proposed actions in light of the above.

2. Background

2.1 Deloitte were engaged by Chris Aujard General Counsel and Lesley Sewell, CIO, at the request of the Board, to conduct a desktop review of certain matters as part of project Sparrow. The terms of reference for the review were based around the following direction provided by the Post Office legal team:

- "POL is responding to allegations from Sub-postmasters that the Horizon IT system used to record transactions in POL branches is defective and that the processes associated with it are inadequate. POL is committed to ensuring and demonstrating that the current Horizon system is robust and operates with integrity within an appropriate control framework"

2.2 Over 100 items of documentation were reviewed by the Deloitte's team who also interviewed management from Atos, Fujitsu, IT, Information Security, Legal and the Finance Service Centre. (Internal Audit was not involved at this stage)

2.3 A detailed (72 page) report has been issued but subject to legal privilege. Management reviews and discussion have since followed. A summary Board Briefing paper has also been issued.

3. Approach

3.1 Deloitte structured its work around a number of key control assertions made by POL over the environment prior to 2010, the changes made to Horizon in 2010 (HNG – X) and the transactions and control environment operating today.

The review considered the risks and controls in the following three areas.

- System Baseline Assurance- original Horizon implementation and 2010 activity.
- IT provision assurance – current IT management activities (security, IT operations, system changes)
- System Usage assurance – Controls around the business processes, their design and operation.

POL00206524

The assertions they considered included the following:

- The system was fit for purpose and worked as intended when first put in.
- Major changes since implementation have not impacted the design features adversely
- Supporting IT processes are well controlled
- Transactions from the counter are recorded completely, accurately and on a timely basis
- Directly posted "Balancing Transactions" are visible and approved
- The Audit Store is a complete and accurate record of Branch Ledger transactions
- Information reported from the Audit Store retains original integrity
- Database administrators (DBAs) or others granted DBA access have not modified Branch Database nor Audit Store data.
- Data posted from other systems and teams is visible to and accepted by sub-postmasters

3.2 The work was desktop and interview based using information that was available to POL and the parties involved. No direct testing of control assertions were made. Deloitte did not test any of the relevant Horizon features and were not required to revalidate the assurance work supplied to them. The exceptional use of the Balancing Transaction process event in 2010 was noted and verbal assertions from Fujitsu relied upon.

3.3 The documentation review included considerable technical information provided by Fujitsu plus third party work assurance undertaken by E&Y (ISAE 3402 report on the Horizon managed service), Bureau Veritas (PCI DSS compliance report on Horizon and ISO 27001) and Royal Mail Internal Audit (Security controls, 2011, 2012. The POL IA team was not in place until June 2013).

4 Key Observations and Findings

4.1 The table below summarises the observations documented on pages 4-5 and 25-26 of the full report.

Strengths	Areas for attention
Technical Horizon system documentation is extensive	Documentation is not in a risk and controls perspective
Audit Store integrity maintained through digital seals and signatures and verification processes during extraction of data from the store.	POL reliance on Horizon features to operate as described limited to the IT provision areas of ISAE3402, PCI DSS and ISO27001. These may be sufficient for the purposes of those standards but may not be enough for full POL reliance over operation of Horizon Features and additional testing may be needed.
Governing controls over key day to day IT management activities independently	Business use of documentation not complete or up to date.

POL00206524

Strengths	Areas for attention
tested.(ISAE 3402)	
Independent reviews (ISAE, 27001, PCI) provide good coverage for Information Security, fair coverage for Information Systems and Change Management	Pre-2010 baseline assurance work not available.

4.2 Recommendations proposed by Deloitte

Deloitte provided detailed recommendations across three areas:

- Actions that may assist project Sparrow.
- Actions for Future Systems requirements.
- Actions for more holistic approach to risk and assurance over Horizon
    - These are detailed in appendix 1.
    - They centre upon improved documentation, specific review of the privileged access controls around Balancing Transactions, detailed analytical testing of historic transactions, system requirements for any new system and a proposal for a holistic programme of risk and assurance for POL's overall risk and control framework.

4.3 These recommendations should be considered by management to consider in light of:

- Overall business risk.
- Risk Appetite.
- Future of the Horizon System
- Current POL Assurance capacity (1st, 2nd and 3rd lines)
- Legal imperatives
    - The work should also be considered in light of POL senior management commitments to 10 priority actions and behaviours (The 10 Accelerators). Whilst these should not take precedence over key risks to information and the Post Office reputation, management will need to judge priorities, capacity and financial resources.
    - Regard should be given to other initiatives being undertaken across the business. (E.g. the risk and change assurance work with PwC).

4.4 The actions that should be taken with respect to these recommendations have been discussed by Legal, Risk, Information Security, Finance Service Centre and Internal Audit.

Ref	Summary of recommendation	Business View
A1	Perform a detailed review of Balancing Transactions use and controls.	Yes.
A2	Perform implementation testing of Horizon features.	Only if resources are available and on agreement of scope.

POL00206524

Ref	Summary of recommendation	Business View
		Consider if can be done by E&Y as part of 3402 testing.
A3	Analytical Testing of Historic Transactions	No. Considered to be a large exercise for which the benefit is questionable.
A4	Update/Create documentation for adjustment and reporting processes at FSC	Yes - but see proposed scope from Head of FSC in appendix.
B1	Produce Future Systems Requirements Document.	At appropriate time when new system is considered.
C1-C4	Risk Workshop, Construct risk and control framework, Test Controls, Ongoing Assurance delivery and pro-active monitoring across Horizon and full POL business.	Head of Risk recommends that C1-C4 should be carried out within the confines of the Horizon system to establish a robust control framework. The wider organisational piece is already being addressed through the existing work of the Risk & Compliance team, and the partnership for strategic assurance activity with PwC. Head of ISAG recommends that current Information Security Assurance activity should also be considered.

5. Required Action

5.1 The Risk and Compliance Committee is required to note the activity that has taken place and support the proposed actions, namely;

- Test of controls around the Balancing Transactions,
- FSC documentation, and
- Risk and control framework around Horizon.

Chris Aujard
General Counsel

POL00206524

Confidential **PAPER TWO**

Appendix 1

Further details of Recommendations from Deloitte.

Ref	Details
A1	**Perform a detailed review of Balancing Transactions use:** Use suitably qualified party independent of Fujitsu to review controls around the need to use the Balancing Transactions functionality, communications with Sub – post masters, reasons for making adjustments and full review of procedures and policies.
A2	**Perform implementation testing of Horizon Features** Use party independent of Fujitsu to conduction implementation testing of Horizon features. Use the review to confirm features are operating as described from documentation.
A3	**Analytical Testing of Historical Transactions** Audit Store documentation asserts the system holds seven years of branch transactions and system event activities. In addition assertions over data integrity, record and field structure and key controls such as JSN sequencing. Not validated by parties outside of Fujitsu. Analytical techniques using modern technology for Big Data sets could allow POL to conduct detailed risk analytics of Audit Store data to verify that the data is as expected and derive other insights or exceptions. This may identify Horizon features that could be automatically monitored.
A4	**Update / create documentation formalised for all key adjustment and reporting processes in operation over Horizon in the FSC.** Identify and document all key activities in the FSC for adjustments to Sub Postmaster ledgers, control activities that reconcile transaction data visible to the Sub-Postmasters to the Audit Store's "High Integrity" copy of Branch Ledger transactions. This can be used to verify the completeness of the Horizon Features in place that have been verbally asserted and perform implementation controls verification in A2.
B1	**Produce Future Systems Requirement Document** Produce system of requirements for any future Horizon platform to deliver against. This should include Key Control objectives, current day control activities. Schedule to include matters that help design preventative, detective and monitoring control activities. Longevity of data retention in Audit Store and cryptographic requirements should be applied.

POL00206524

Ref	Details
C1	**Risk Workshop.** Conduct an exercise with Key Stakeholders in POL to create baseline understanding of risk and risk management concepts, share examples of other companies, and determine how POL can become more risk intelligent organisation.
C2	**Construct a risk and control framework** Extend and confirm the completeness of the Horizon Features and use the framework to prioritise areas for improvement. Extend the framework to POL's overall risk and control framework, not just those areas relevant to Horizon
C3	**Test Controls.** Use the framework to test controls across POL's risk environment. Use a third party to operate against a recognised assurance standard.
C4	**Sustain Assurance Delivery and Implement more proactive monitoring.** Longer term assurance map to sustain assurance delivery for POL over key risks. Consider continuous controls monitoring using automated alerts if key behaviours in the system are identified.

Proposed alternative actions for A4 – Rod Ismay Head of FSC

Ensure comprehensive documentation of:

- Key processes in FSC which identify or respond to accounting issues in branches
- Key controls in the data pipeline from point of sale to central finance systems

This can then be used to provide assurance as to the processes and controls around data transmitted from Horizon and around corrections notified to Sub postmasters.

<u>Reasons for revised proposals:</u>

The FSC does not directly make adjustments to Sub-postmaster ledgers. Instead it identifies or responds to issues and then sends Transaction Corrections to branches such they are able to see and satisfy themselves about changes.

Data is held in very different structures in different places which would make the reconciliation proposed by Deloittes a challenge and may not be beneficial or time efficient

The branch has data in a trial balance list. The audit store has individual transactions. The FSC will have data batched by client to drive the settlement runs.

- Therefore an action can be to update documentation of the data harvesting and interface checks down the pipeline and control testing down that pipe. That could help test the completeness, timeliness and accuracy of data moving down the pipe.

POL00206524

Confidential **PAPER THREE**

RISK AND COMPLIANCE COMMITTEE

Business Continuity Proposal

1. Purpose

The purpose of this paper is to:

- Provide the committee with an update on the actions requested at the last meeting, to review the proposals in the light of project Sparrow and to consider testing arrangements; (see section 4);

- Provide the Risk and Compliance Committee with proposals for the enduring model for business continuity at Post Office and seek a decision regarding the enduring resourcing model; and

- Propose an expansion of the responsibilities of the Business Continuity Steering Group (BCSG), taking ownership of major incident management and crisis management.

This paper follows up from the last Risk and Compliance Committee meeting in May 2014.

2. Business Continuity at Post Office

During previous external and internal audits in 2012, it was identified that a greater level of assurance of business continuity (BC) at Post Office is required. There are a number of key drivers that support the requirement for business continuity capability and management:

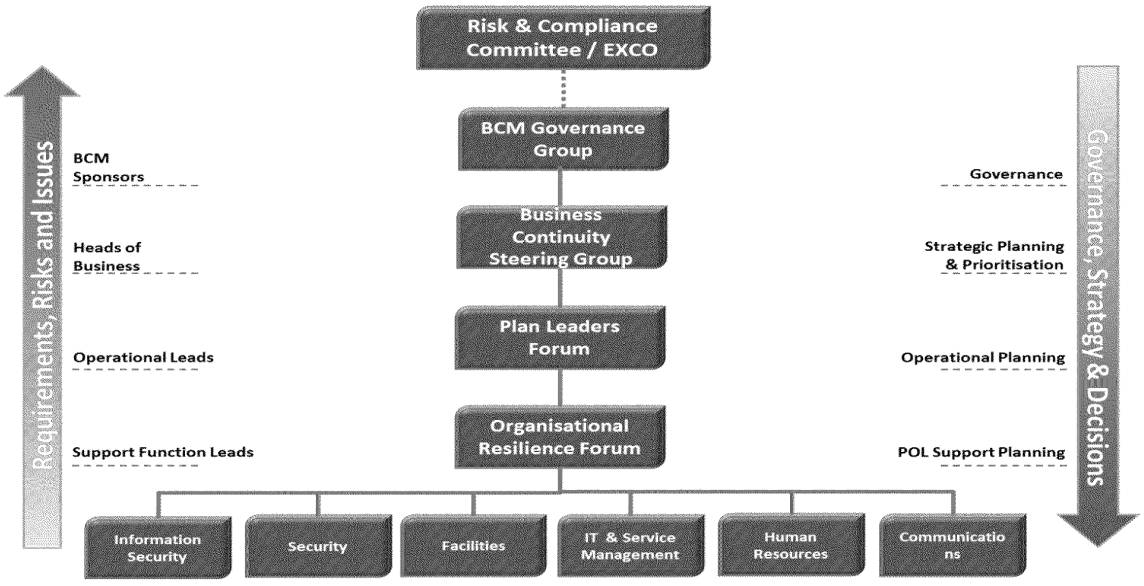
- business resilience and capability,
- protecting Post Office brand and reputation,
- satisfying contractual requirements for Post Office clients,
- managing Post Office's third party dependencies and supply chain,
- reducing impact and cost of interruption,
- managing Business Continuity and Disaster Recovery risks,
- government obligations,
- business growth and change, and
- separation, transformation, new bids, products, & services etc.

In response to the business continuity requirements, a programme of work has been initiated to develop a Business Continuity Management System (BCMS) framework, support business change and mature capability within the business.

2.1 Business Continuity Governance

Post Office requires enduring ownership, governance and technical capability to ensure effective business continuity management and delivery. The governance for business continuity has previously been agreed and is demonstrated in the diagram below.

POL00206524



The Business Continuity Steering Group (BCSG) takes ownership for business continuity and has membership from each directorate, nominated by their executive member. Each member is responsible for ensuring the delivery of any business continuity requirement as per Post Office Policy.

The BCSG reports directly to the Risk and Compliance Committee to give assurance that the business continuity threats and risks have the appropriate system of management and where required, planning and mitigation.

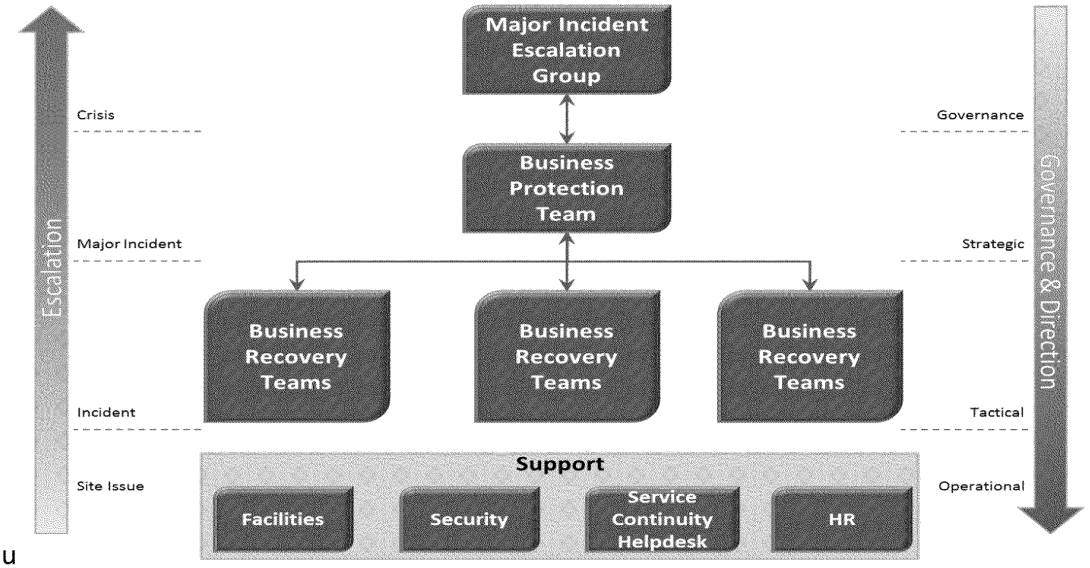
Supporting the BCSG will be a network of plan leaders who are responsible for business continuity plans and business recovery teams for their business area, site or service. These recovery teams, headed by plan leaders will support the day to day planning and manage incidents for their allocated areas and form a virtual community across Post Office. Each plan leader is accountable to the BCSG members for their directorate.

This agreed approach benefits Post Office, as detailed below:

- business owned and accountable business continuity,
- a network of stakeholders skilled to support BC for their designated area,
- resource and cost effective BC management,
- key business points of engagement for the BC Manager and resources to support,
- delivery of BC cultural, training and awareness throughout the business,
- development of capable recovery teams providing resilience and succession planning through the assignment of appropriate recovery team roles,
- capability to isolate and effectively manage incidents through business recovery teams or escalate and support major events with a defined and capable structure,
- a reviewed and updated incident and crisis response structure,
- the effectiveness of the BCSG taking ownership for major incident and crisis management combined with BCMS governance, and
- providing an updated business protection team (BPT) comprised of the BCSG members.

POL00206524

Incident management governance is outlined below:



u

2.2 Business Continuity Resourcing

In order to maintain effective business continuity within Post Office and support the above, an appropriate resourcing model is required. The programme has reviewed a number of options and seeks approval in principle for an option to be fully documented and presented to the committee at its next meeting.

Post Office requires business continuity to provide a number of services and activities that ensures the appropriate preparedness, capability and commercial benefit. These include:

- management and development of the BCMS Framework,
- support and guidance to the BCSG and ExCo,
- development of Post Office BC Plans,
- delivery of client business continuity obligations,
- project support, guidance and governance,
- commercial and procurement support, guidance and governance,
- management of BC threats and risks,
- government BC obligations,
- development and ownership of crisis and incident management, and
- support, guidance and governance for transformation, growth and business change.

2.3 Resourcing Model Options

A number of options have been reviewed based on Post Office requirements, planned business change and projected growth and are presented in the tables on the following page:

POL00206524

Option	Hybrid - (BCM POL with External Support) – Recommended Option
Headcount / Resource Profile	Recruitment of a full time Business Continuity Manager and a provision for external support and expertise
Synopsis	Recruitment of the BCM and continuation of external support to report to Head of Risk Governance. • Central Point for BC management of the BCMS Framework • Delivery of BC Policy and Framework currently owned by Risk Governance
Benefits	• Ensures the delivery of Business Continuity and the appropriate business support from BC • Develops BCM management resource • Continued focused delivery from skilled resources • Low headcount that is easily reduced over time as BCMS matures or business change reduces • External support with skills to deliver and mature BCMS • Business requirements supported effectively and efficiently • Combining business knowledge with technical skills for optimum result • Enduring solution with flexibility and contingency • Benefit of learning's from other organisations that best suits POL culture • Most cost effective (benchmarked) • Lower risk based option ensuring continuity of Post Office Business Continuity • Centralised point to monitor and manage BC threats and risks • Skilled resources to continue development of commercial BC opportunities
Drawbacks	• Present unbudgeted costs NB: Possibility of centralisation of Business Continuity current spending in different business areas. To be finalised on agreement of option in principle.

Options	Business Continuity Team	Managed Service (External)
Headcount / Resource Profile	Recruit and develop a full Business Continuity Team	Appoint a outsourced provider to fully manage Business Continuity for the Post Office
Synopsis	Recruit a BCM Team • Business Continuity Manger • Business Continuity analysts and specialists • Business Continuity Testing and Exercising resource	Appoint a outsourced provider to fully manage Business Continuity for the Post Office • Managed services through a framework agreement / contract • Continuation of current contracted services with increase manpower to support growing business requirements
Benefits	• Development of Internal BC Team • Continuity within POL • Large base of skilled resources	• Skilled proven resources • Focused delivery • Low headcount • Resources can be reduced quickly (with risk)
Drawbacks	• Fixed Headcount & cost • Time and cost to mature staff to the appropriate level • Risk of cycle of churn once staff are matured and can seek higher paid employment outside the Post Office • Lack of POL skilled staff to appoint • Reduction difficult if BCMS requirement reduces • Ineffective business support and increased risk	• Highest cost model • Resources not easily reduced as BCMS matures (no POL staff to hand over to) • No enduring Post Office Business Continuity capability

POL00206524

Of the three approaches above, the hybrid model is the preferred option of the business continuity programme as providing the best value for money and the most flexibility
.

3. Incident Management

With the transition of the IT Service Desk to ATOS, a gap has been identified in relation to the appropriate ownership of incident and crisis management at Post Office. Additionally, the business protection team (BPT) membership is out of date and a membership review is required.

Based on the role of the Business Continuity Steering Group (BCSG) in developing and managing business continuity and the supporting structures for incident response, it would be prudent, and is recommended, that this group takes ownership of major incident management and crisis management. The BCSG members would now form an updated business protection team (BPT) and create a forum to both govern and respond to major events.

The Head of Risk Governance, Business Continuity Manager and Head of IT Services have reviewed this option and fully support the transition to the BCSG.

4. Risk and Compliance Committee Action: May 2014

The committee requested the BCM paper to be brought back to the next meeting with clarification and consideration of work being performed by Belinda Crowe and consideration to how the proposed future model is to be tested.

Business Continuity met with Belinda Crowe and clarified that the BCMS (Business Continuity Management System) will include a robust review of the Crisis Management response and also includes Crisis Management exercises to validate planning and preparedness. Sparrow does not have this in scope and it is appropriate for Business Continuity to manage these activities. This will ultimately be owned by the BCSG (Business Continuity Steering Group) as suggested in the paper. This meets the considerations from Sparrow and ensures adequate testing of the both the Major and Crisis Management response.

5. Recommendations

The committee is asked to:

- determine, in principle, the resourcing model to be implemented,
- agree that the business continuity programme will present this option in detail, including costs, at the next committee meeting, and
- support the BCSG in taking ownership of crisis and major incident management for Post Office.

POL00206524

Post Office Ltd – Confidential PAPER FOUR

Risk and Compliance Committee (R&CC)		Reference: R&CC/MIN/MAY14
Date: 29th May 2014	**Venue: Boardroom, 148 Old Street, London**	**Time: 10.00 – Noon**
Attending:		
Chris Aujard	General Counsel	Chair
Alwen Lyons	Company Secretary	Member
Paula Vennells	Chief Executive Officer	Member
Colin Stuart	Head of Commercial Finance	Member (for Chris Day)
Neil Hayward	Group People Director	Member
Martin Edwards	Chief of Staff	Report
David Mason	Head of Risk & Compliance	Report
Fay Healey	Head of HR	Report
Ian Kennedy	General Manager Network Transformation	Report
Rob Bolton	Assurance Adviser	Secretariat
Apologies:		
Chris Day	Chief Finance Officer	Member

Introduction

Purpose

The chair outlined the key themes from the papers and the format of the meeting

Discussion

The chair welcomed everyone to the meeting and outlined the key themes from the supporting papers as:

- Risk maturity and a more pragmatic business approach to risk management
  Assurance around transformational change
- Business continuity
- Anti-Money Laundering (AML)
- Risk acceptance

The committee agreed the key themes and to focus the meeting on these areas

Agenda Item 1

Head of Risk Report

Purpose

The committee discussed the Head of Risk report focusing on the areas highlighted at the meeting

Discussion

The progress made in developing the risk management framework was reported to the committee. It was confirmed that the understanding of risk management in the business was being developed by the Risk Business Partner model through the hearts and minds approach. It was agreed by the committee that it would be useful to understand the current Business Partner structure and how the model operates in the business.

The committee considered the performance of compulsory corporate training and where the ownership of this sits in the business. A paper was requested identifying all the regulatory and compulsory training requirements for the business, including details of when this training had last been carried out. It was agreed that ownership of compulsory training needed to be established for the organisation. Linking the completion of compulsory training to bonus payments was also discussed and it was agreed that once the business owner and training landscape had been determined this could be further assessed.

The risk events were discussed and the committee asked for confirmation that the big machines event did not have any impact on Subpostmasters or Project Sparrow. The committee endorsed the content of the paper and it was agreed that the failure of external bank IT systems should be investigated as a potential risk event to be included in future papers.

Emerging risks were considered and the committee identified some further emerging risks:

POL00206524

Post Office Ltd – Confidential PAPER FOUR

- Cyber security
- Withdrawal of state aid

It was confirmed that the owner of the Scottish independence risk should be Mike Granville and that a related paper recently completed should be circulated to committee members. The committee discussed the status of Financial Conduct Authority (FCA) approved persons in the business and it was agreed that there should be further Post Office approved persons and that regular training should be provided.

The recently finalised Xanadu report was discussed and the committee agreed that there should be accountability identified for each of the recommendations in the report and also a single owner of the report accountable for the delivery of all the actions. The committee agreed that to prevent a similar situation happening again it was important for the lessons learned from the review to be built into the risk assessments performed for other projects and programmes. Failure Point Analysis to be performed on Project Wave and Project Ivy which would then be rolled out as benchmarks for future projects. The committee requested that the Commercial Director attend the next meeting in July to provide assurance on the delivery of Project Wave.

The performance of interim post implementation reviews (PIRs) throughout the life of a project was also discussed by the committee.

Outcomes

The committee received the Head of Risk report and identified a number of further actions

Actions

Ref	Action	Lead	By
1582	Circulate a report to the committee identifying the Risk Team structure/resource and how the Business Partner model works	David Mason	Circulate by email – 20th June 2014
1583	Risk & Compliance team perform a survey to identify the compulsory/obligatory corporate training that is required to be completed and identify any gaps in actual training that has been completed	David Mason	Next meeting
1584	Discuss and agree with Group People Director how any gaps in compulsory training are resolved	David Mason	Next meeting
1585	Confirm that Big Machines risk event does not have any implications on Subpostmasters and Sparrow	David Mason	Confirm by email – 6th June 2014
1586	Failure of external bank IT systems to be investigated to determine exact nature of failures and if connected to Bank of Ireland systems. To be reported within risk events paper if appropriate	David Mason	Next meeting
1587	Include the following as new emerging risks: • Withdrawal of state aid • Cyber security	David Mason	Next meeting
1588	Scottish independence emerging risk owner to be changed to Mike Granville and related paper circulated to the committee members	David Mason	20th June 2014
1589	Assess the options for further FCA approved persons within Post Office and identify training requirements.	David Mason	Next meeting
1590	Specific names to be identified for the actions from the Xanadu assurance review	David Mason	Confirm by email – by next meeting
1591	Single accountable person be identified for ensuring all the actions from the Xanadu review are delivered	David Mason	Confirm by email – by next meeting
1592	Discuss with Alison Thompson how lessons from Xanadu can be built into risk assessments performed for projects and programmes	David Mason	Next meeting
1593	Risk team to raise any concerns noted in projects and programmes similar to that identified in Xanadu review	David Mason	Next meeting
1594	Commercial Director to be invited to the next meeting to provide the committee with assurance on delivery of Project Wave	David Mason	Next meeting
1595	Failure Point Analysis to be performed on Project Wave and Project Ivy and results used as a benchmark for future projects	David Mason	Next meeting

POL00206524

Post Office Ltd – Confidential PAPER FOUR

1596	Discuss with Alison Thompson interim Post Implementation Reviews being performed throughout the life of a project rather than at the end	David Mason	Next meeting

Agenda Item 2

TUPE transfer to ATOS

Purpose

The committee reviewed the TUPE paper and considered the identified lessons learned

Discussion

The committee received the paper that had been submitted and considered the lessons learned from the transfer and how the actions raised in the paper would be delivered. It was identified that some of the actions raised in the paper would be built into a framework to be applied to future change activity and the committee requested an update be provided to the next meeting identifying how the actions raised in the TUPE paper were going to be managed and delivered.

Outcomes

The committee received the TUPE paper and requested a further update on the actions raised

Actions

Ref	Action	Lead	By
1597	Provide the committee with an update on how the actions raised in the TUPE paper are going to be delivered	Fay Healey	Next meeting

Agenda Item 3

Anti-Money Laundering (AML) Risk Assessment

Purpose

The committee reviewed the AML risk assessment and the status in Post Office

Discussion

The Anti-Money Laundering (AML) risk assessment was presented to the committee and it was confirmed that this had been produced following a gap raised from an independent review of AML process in Post Office. It was identified that whilst there were good controls relating to some products, particularly travel money, they were not future proof. The committee requested that the paper be re-issued with the business position against the different products in the risk assessment presented in tabular form. The Head of Risk was asked to produce the job specification for the Money Laundering Reporting Officer (MLRO) that would be required for the future state of Post Office.

Outcomes

The committee received the update on the status of assurance activity.

Actions

Ref	Action	Lead	By
1598	AML paper to be re-issued identifying the business position against each of the products in tabular form	David Mason	20th June 2014
1599	Discuss with the Horizon development team the AML requirements to be captured for regulated products	David Mason	Next meeting
1600	Produce and circulate the job specification for the MLRO	David Mason	Next meeting

Agenda Item 4

Risk Acceptance & Exception to Acceptable Use Policy

Purpose

The committee reviewed the new risk acceptance procedure and considered an exception to the acceptable use policy

Discussion

The new risk acceptance procedure was discussed together with the risk acceptance associated with the

POL00206524

Post Office Ltd – Confidential PAPER FOUR

exception to the acceptable use policy. The risk acceptance procedure was agreed by the committee including the role of the committee in the process however the exception to the acceptable use policy was not agreed. It was requested that benchmarks or examples of how other businesses manage the exception to the acceptable use policy be collated and provided to the committee.

Outcomes

The committee agreed the risk acceptance procedure, including the role of the committee in the process.
The committee did not agree the exception to the acceptable use policy

Actions

Ref	Action	Lead	By
1601	Benchmarks or examples of how other businesses manage the exception to the acceptable use policy to be collated and provided to the committee	Julie George	3rd July 2014

Agenda Item 5

Business Continuity Proposal

Purpose

The committee was asked to agree the business continuity enduring model proposal

Discussion

A Business Continuity (BCM) paper had been submitted identifying three proposals for the enduring model of BCM in Post Office including where it would sit in the business and how it would be managed.

The committee requested that the paper be returned to the next meeting to include links to the work being performed by Belinda Crowe and also consideration to how the proposed future model is to be tested.

Outcomes

The committee did not agree a business continuity proposal and requested further information

Actions

Ref	Action	Lead	By
1602	BCM paper to be brought back to the next meeting with links to the work being performed by Belinda Crowe and consideration to how the proposed future model is to be tested	David Mason	Next meeting

Agenda Item 6

Network Transformation Risk Maturity

Purpose

The committee was asked to receive an update on risk management activity and maturity within the Network Transformation programme

Discussion

The Network Transformation (NT) deep dive was not performed by the committee however the General Manager Network Transformation was asked to provide a short summary of the risk activity being performed and the risk maturity within the programme.

It was identified that the programme when measured against the Portfolio, Programme and Project Maturity Model (P3M3) was rated as between 1 and 2 on the scale of maturity (1 being the lowest). The committee requested that a risk mapping exercise for all the NT risks be performed and a proposal provided to the committee on how this can fit an enterprise risk model for the business. The committee also requested sight of a presentation relating to the mapping of risks within projects and programmes

Outcomes

The committee did not perform a deep dive on the NT risk
The committee received an update on risk activity within the programme and requested further information

Actions

Ref	Action	Lead	By

POL00206524

Post Office Ltd – Confidential PAPER FOUR

1603	Risk mapping exercise for all the NT risks to be performed and proposal provided to the committee on how this can fit an enterprise risk model for the business	Ian Kennedy	Next meeting
1604	Provide the committee with the dirty presentation relating to mapping of risks within projects and programmes	Ian Kennedy	Next meeting

Agenda Item 7

Minutes & Matters Arising

Purpose

The committee was asked to agree the previous minutes and receive the updates on actions to confirm completion.

Discussion

The committee agreed the minutes from the last meeting in March 2014 and all actions were confirmed as completed. Actions raised in future minutes to identify timescales for delivery.

Outcomes

The committee agreed the minutes from the previous meeting.
The committee agreed that all previous actions had been closed.

Actions

Ref	Action	Lead	By
1605	Actions in the minutes to identify timescales for delivery	Rob Bolton	Issue of minutes

Agenda Item 8

Any Other Business

Purpose

The committee to consider any other business not captured on the agenda and any necessary actions.

Discussion

No AOB was raised

Outcomes

None

Actions

Ref	Action	Lead	By
None			

Rob Bolton
Risk & Assurance Adviser
16th June 2014

Action Summary and Updates

Ref	Action	Lead	By	Update

POL00206524

Post Office Ltd – Confidential PAPER FOUR

1582	Circulate a report to the committee identifying the Risk Team structure/resource and how the Business Partner model works	David Mason	Circulate by email – 20th June 2014	Circulated with meeting papers
1583	Risk & Compliance team perform a survey to identify the compulsory/obligatory corporate training that is required to be completed and identify any gaps in actual training that has been completed	David Mason	Next meeting	An initial list has been compiled and is being reviewed with key stakeholders (eg. Security, H&S) in the business.
1584	Discuss and agree with Group People Director how any gaps in compulsory training are resolved	David Mason	Next meeting	This will be taken forward once the output from action 1583 has been confirmed
1585	Confirm that Big Machines risk event does not have any implications on Subpostmasters and Sparrow	David Mason	Confirm by email – 6th June 2014	Confirmation provided by email that no implications on Subpostmasters or Sparrow - Big Machines only support three web based applications and the reference data and database is completely segregated and not linked to Horizon - action completed
1586	Failure of external bank IT systems to be investigated to determine exact nature of failures and if connected to Bank of Ireland systems. To be reported within risk events paper if appropriate	David Mason	Next meeting	This is being progressed with the Bank of Ireland Group technology and change team and we are currently awaiting their response.
1587	Include the following as new emerging risks: • Withdrawal of state aid • Cyber security	David Mason	Next meeting	Included in Head of Risk report for July meeting – action completed
1588	Scottish independence emerging risk owner to be changed to Mike Granville and related paper circulated to the committee members	David Mason	20th June 2014	Confirmed that paper circulated to ExCo members which includes all of the R&CC members - action completed
1589	Assess the options for further FCA approved persons within Post Office and identify training requirements.	David Mason	Next meeting	We have been working with the Bank of Ireland to assess whether the FCA rules in respect of Approved Persons continue to be deployed appropriately with respect to the Post Office. The Bank's regulatory team is currently of the view that as an Appointed Representative with our range of Financial Services activities we would be required by the FCA to have the 'governing functions' notified as Approved Persons. The FCA definition of 'governing functions' covers both the CEO, who will still be seen as the pre-dominant executive, together with all the main Board directors (executive and non-executive). The FCA handbook rules do not allow any scope for any other members of the Post Office executive team or other senior staff or control functions to be Approved Persons under the Appointed Representative

POL00206524

Post Office Ltd – Confidential PAPER FOUR

				arrangements.
1590	Specific names to be identified for the actions from the Xanadu assurance review	David Mason	Confirm by email – by next meeting	Update included in assurance activity section of Head of Risk report
1591	Single accountable person be identified for ensuring all the actions from the Xanadu review are delivered	David Mason	Confirm by email – by next meeting	Update included in assurance activity section of Head of Risk report
1592	Discuss with Alison Thompson how lessons from Xanadu can be built into risk assessments performed for projects and programmes	David Mason	Next meeting	This action has now been overtaken by the sourcing of a strategic assurance partner
1593	Risk team to raise any concerns noted in projects and programmes similar to that identified in Xanadu review	David Mason	Next meeting	Action completed
1594	Commercial Director to be invited to the next meeting to provide the committee with assurance on delivery of Project Wave	David Mason	Next meeting	A group of SLT members has been convened to provide oversight and assurance over Project Wave
1595	Failure Point Analysis to be performed on Project Wave and Project Ivy and results used as a benchmark for future projects	David Mason	Next meeting	This action has now been overtaken by the sourcing of a strategic assurance partner
1596	Discuss with Alison Thompson interim Post Implementation Reviews being performed throughout the life of a project rather than at the end	David Mason	Next meeting	This action has now been overtaken by the sourcing of a strategic assurance partner
1597	Provide the committee with an update on how the actions raised in the TUPE paper are going to be delivered	Fay Healey	Next meeting	Confirmation received that all actions have owners and timescales and these are being monitored.
1598	AML paper to be re-issued identifying the business position against each of the products in tabular form	David Mason	20th June 2014	Action completed. Paper re-issued to members 9th July by email.
1599	Discuss with the Horizon development team the AML requirements to be captured for regulated products	David Mason	Next meeting	Initial conversation with Spencer Chapman and this to be followed up
1600	Produce and circulate the job specification for the MLRO	David Mason	Next meeting	The MLRO job specification is being finalised and will be circulated by email prior to the meeting.
1601	Benchmarks or examples of how other businesses manage the exception to the acceptable use policy to be collated and provided to the committee	Julie George	3rd July 2014	Work in progress – awaiting feedback from industry bodies.
1602	BCM paper to be brought back to the next meeting with links to the work being performed by Belinda Crowe and consideration to how the proposed future model is to be tested	David Mason	Next meeting	Business Continuity completed a session with Belinda Crowe and clarified that BCMS (Business Continuity Management System) will include a robust review of the Crisis Management response and also includes a Crisis Management exercise. Sparrow does not have this in scope and it is appropriate for Business Continuity to manage these activities. This will ultimately be owned by the

POL00206524

Post Office Ltd – Confidential PAPER FOUR

				BCSG (Business Continuity Steering Group) as suggested in the paper. The committee is requested to approve the paper and Business Continuity will proceed with the above and additional Business Continuity activities.
1603	Risk mapping exercise for all the NT risks to be performed and proposal provided to the committee on how this can fit an enterprise risk model for the business	Ian Kennedy	Next meeting	Agenda item at July meeting
1604	Provide the committee with the dirty presentation relating to mapping of risks within projects and programmes	Ian Kennedy	Next meeting	Agenda item at July meeting
1605	Actions in the minutes to identify timescales for delivery	Rob Bolton	Issue of minutes	Action completed

POL00206524

Confidential **Action 1582**

RISK AND COMPLIANCE COMMITTEE

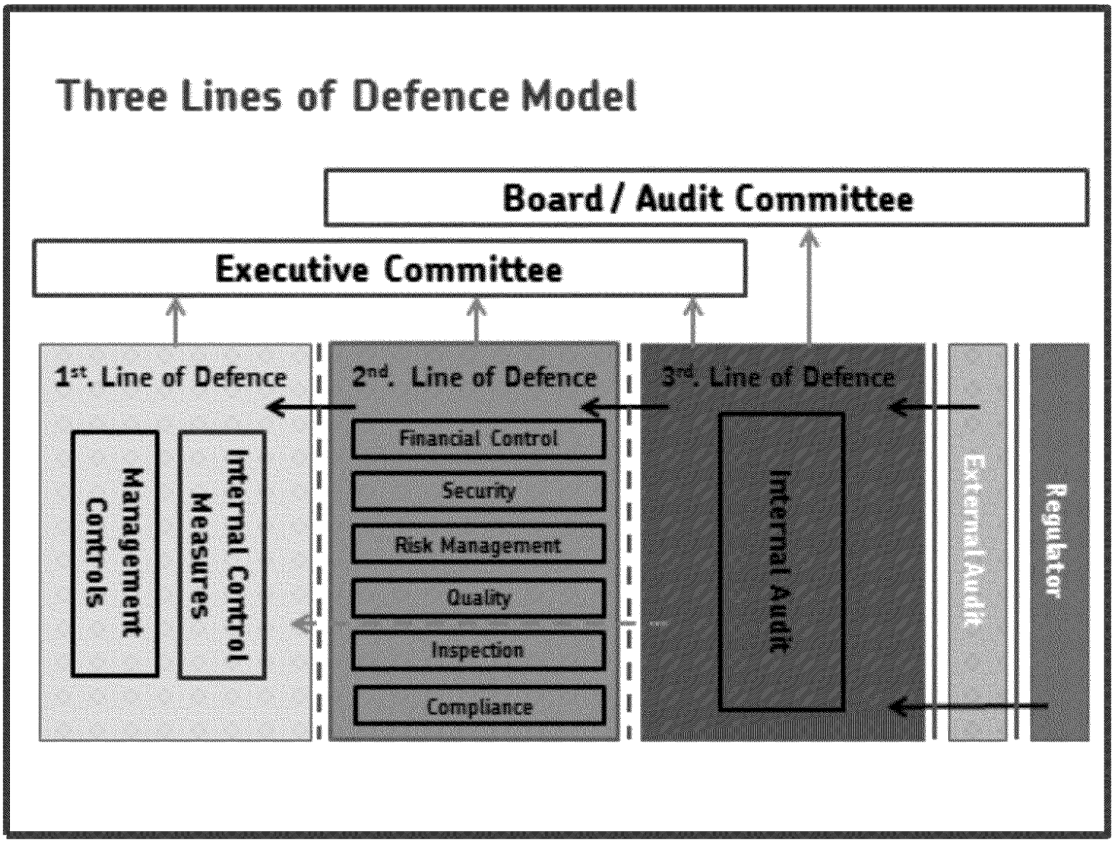
Risk Team Structure and Business Risk Partner Model

1. Purpose

The purpose of this paper is to respond to the committee's request for a report on the Risk Team structure, resources and the business partner model.

2. Overall Structure

The structure of risk management at the Post Office is based on the "three lines of defence" model, used in the majority of organisations regulated by the UK Financial Conduct Authority and summarised below:



Based on: Institute of Internal Auditors Position Paper - The three lines of defence in effective risk management and control

POL00206524

This model has been implemented at Post Office as follows:

- **1st Line** The business units own and manage risk. They are responsible for maintaining effective internal controls and for executing risk and control procedures on a day-to-day basis. Management identify, assess, and respond to risks, ensuring that activities are consistent with goals and objectives;

- **2nd Line** The risk team provides oversight and challenge of risk management activities in the first line. The risk team are responsible for delivering the Post Office's risk management strategy, creating a culture and framework within Post Office in which the management of risk is an integral part of decision making and sound risk-based decisions are encouraged and rewarded; and

- **3rd Line** The internal audit team provides independent assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the first and second lines of defence achieve risk management and control objectives.

3. The Risk Team

The risk team, led by the Head of Risk Governance, consists of:

- Five business risk partners, sharing knowledge and expertise of risk with the business units, supporting the deployment of the risk framework in the first line, reviewing and challenging risk management outputs and advising on all aspects of day to day management of risk;

- A business risk and assurance team building the risk framework, assuring its effectiveness and providing risk oversight information to the Executive and Board; and

- An anti money laundering manager and assistant fulfilling the Post Office's legal obligation to combat, monitor and report suspected money laundering activity. The Head of Risk Governance is the nominated Post Office Money Laundering Reporting Officer.

An organisational design showing the make-up of the team and the alignment of the risk business partners to the business units is in the appendix.

.

POL00206524

4. Business Partner Role

The risk business partners deliver the hearts and minds approach by being the front line advocates of risk management in the Post Office. Their objective is to work in partnership with the business units to deliver the Post Office's risk management strategy.

This involves:

- oversight of the risk framework,
- advising on product design and business change,
- challenging first line risk management and reporting,
- developing a mature risk management culture,
- providing expert and professional advice, and
- leading improvements in risk management.

The first priority of the risk management strategy and the business partners is to focus on the basics and build a self-sustaining level of risk management competence in the business by:

- advising on specific issues,
- overseeing project and programme risk,
- supporting and facilitating risk identification and assessments,
- helping build risk into business processes and deliverables, and
- assisting the business units in building and using the tools they need to manage risk.

These activities are focussed on helping business units to build their knowledge, skills and awareness of risk management. They are designed to improve the generally low levels of risk management maturity across the Post Office while implementing the risk management strategy across the organisation.

5. Business Risk and Assurance Team

The business risk and assurance team's primary responsibility is to deliver the components of the risk management strategy, while providing accurate and complete management information on the operation of risk management in the Post Office.

This is being achieved by:

- supporting the business risk partners and the risk and compliance committee,
- building the risk framework,
- developing risk management standards, protocols and tools,
- monitoring the risk management strategy,
- monitoring compliance with risk related policies,
- maintaining central risk registers
- assuring the effectiveness of the framework,
- assisting the business in ensuring control effectiveness,
- performing investigations into risks and risk events,
- analysing and collating risk and control data,
- developing an aggregate view of Post Office risk, and
- providing risk oversight information to the Executive and Board.

POL00206524

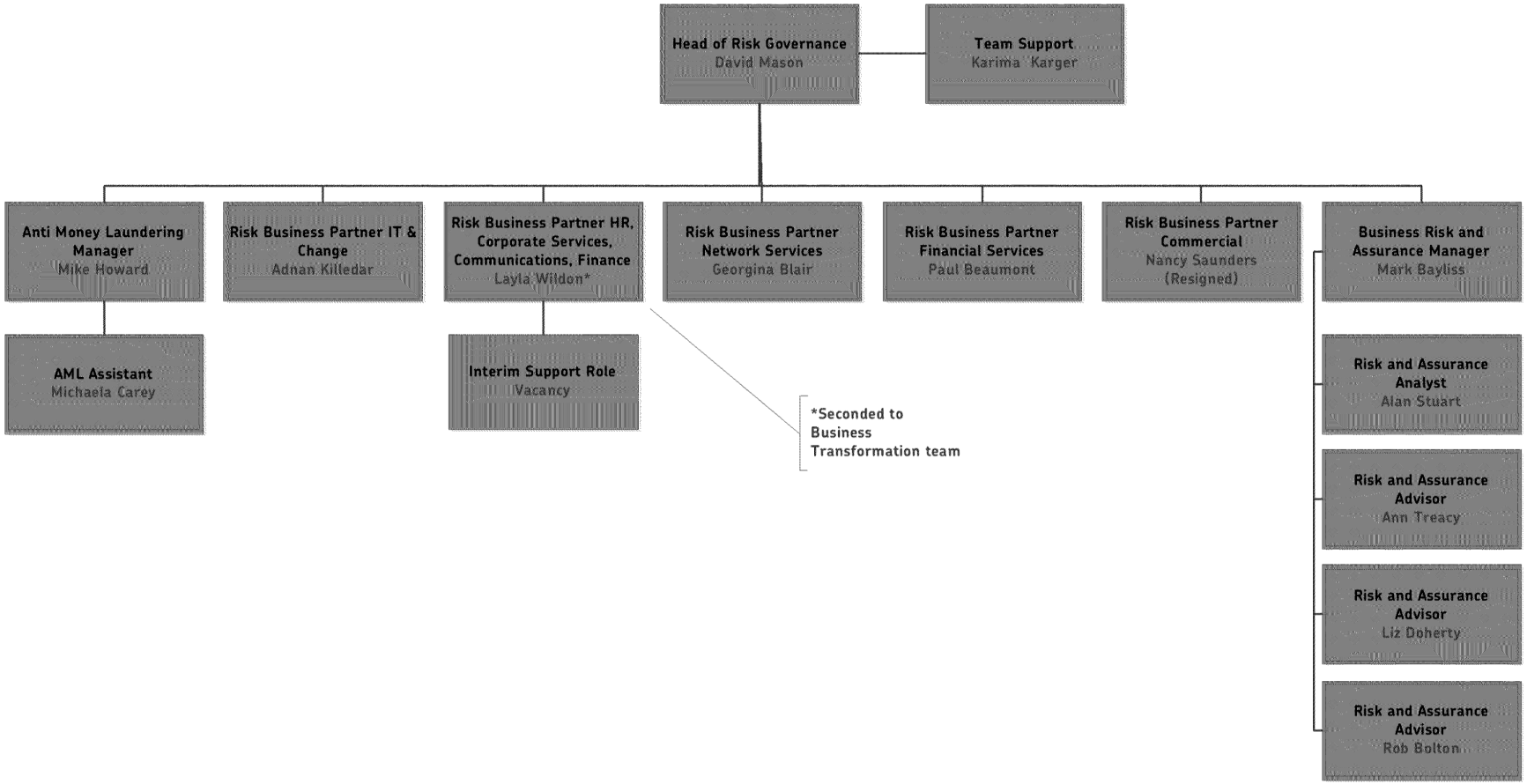
Many of these activities are themselves being developed, refined and improved as part of Post Office risk management strategy, supporting the journey to an embedded and mature risk management culture.

David Mason
26th June 2014

POL00206524

Appendix Action 1582

Risk Team



Risk Team Structure

David Mason
26th June 2014

Appendix

POL00206524

Confidential **PAPER FIVE**

RISK AND COMPLIANCE COMMITTEE

Risk & Compliance Committee Interim Meetings Proposal

1. Purpose

The purpose of this paper is to provide the committee with a proposal for interim meetings outside of the already agreed schedule.

2. Background

It was raised at the meeting on 29th May 2014 that the Risk & Compliance Committee meeting schedule is changed from every two months to monthly.

3. Proposal

A move to monthly full meetings would have a significant impact on the diaries of committee members.

It is therefore proposed that rather than having a full meeting every month the committee is convened monthly for no more than one hour, focussing primarily on new risk events and action updates. Where possible any updates will be communicated by email.

4. Recommendations

The committee is asked to agree the proposal for interim meetings outside of the current schedule.

David Mason
21 July 2014