POL00423307

Internal Audit
Risk and Compliance Committee Report
September 2015

POL00423307

Post Office Internal Audit RCC Report – September 2015

1. Audits completed since last RCC.

Audit	Key Findings	Status (01/09)
Contract Management	• Supplier contract portfolio is not fully known. • Contract Management Framework (CMF) remains in draft (since its development in 2012) and requires further development, finalisation and implementation. • Staff have the ability to define their own roles and responsibilities. • Management are unable to effectively foresee and manage expiration of contracts. • Analysis and management of risks to drive contract management.	• Final Report issued (see Appendix 1). Actions will be followed up with management as appropriate.
Financial Crime	• Staff are not clear on where and how to report suspicions or concerns. • Effective mechanisms to prevent and detect fraud and corruption are not incorporated into policies, procedures and systems. • Focus of proactive / reactive activity is directed towards customers and customer facing areas of the business. • There is no corporate / PO wide approach.	• Report discussed with relevant management and actions agreed (see Appendix 2).

POL00423307

Post Office Internal Audit RCC Report – September 2015

2. Work in progress.

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

POST OFFICE

POL00423307

Post Office Internal Audit RCC Report – September 2015

2. Work in progress cont.

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

POL00423307

Post Office Internal Audit RCC Report – September 2015

3. What we will do - Next 3 months.

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

POL00423307

Post Office Internal Audit RCC Report – September 2015

4. Other matters.

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

POL00423307

Post Office Internal Audit RCC Report – September 2015

4. Other matters cont.

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

POL00423307

Overdue actions from audits

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

POST OFFICE®

POL00423307

Overdue actions from audits

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

POST OFFICE®

POL00423307

Appendix 1 – Contact Management

POL00423307

Contract Management

Internal Audit Report

August 2015

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

POL00423307

Audit Highlights

Background

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

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

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

Assessment

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

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

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

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

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

Key issues

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

Priority actions

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

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

POL00423307

CONTRACT MANAGEMENT

APPENDIX A – PWC Framework

Best Practice

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

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

POL00423307

Appendix 2 – Financial Crime

POL00423307

Financial Crime

Internal Audit Report
September 2015

Executive Responsible:	Jane MacLeod, Alistair Cameron	Prepared By:	Deana Herley – Internal Audit Manager
Distribution:	Neil Haywood John Scott, Sally Smith	Reviewed By:	Garry Hooton – Acting Head of Internal Audit Jane MacLeod John Scott, Sally Smith Angela Van-Den-Bogerd

POL00423307

FINANCIAL CRIME

Background

Financial crime risk is defined as the vulnerability, or exposure of the organisation towards financial crime and irregularity. The prevention, detection and resolution of financial crime is a management responsibility and the business must satisfy itself that it exercises suitable control over 'financial crime risk' covering Head Office functions, corporate services, network, depots and branches. Before separation RMG was responsible for fraud risk management.
The focus of our review has been on the financial crime of fraud. Further reviews of anti-money laundering, bribery and corruption and cyber will be considered as a part of our on-going review of Internal Audit Plan for 2015/16.

Our overall assessment

PO currently has a culture where not knowing what you don't know is accepted. To be confident in conclusions over fraud risk maturity, PO will need to ascertain what it does not know, and how it will go about learning it. As a first step, PO will need to determine its fraud risks organisation-wide and how effectively they are being managed. GE will also need to determine the ideal future state, commission a gap analysis, and prioritise activities that will help to enable the development of an organisation-wide anti-fraud programme. Fraud risk will need to be owned at the top to set the right tone. Ethical behaviours will also need to be communicated to staff, given the lack of clarity noted during the review. Such a programme will not only help to enable appropriate compliance with regulatory mandates, but will also help PO align its behaviours, values and performance drivers as well as, protecting its assets and reputation. The current culture will be hard to change and will require a focused and coordinated approach as well as investment. A sound ethical culture and effective system of internal control will be essential elements for building an anti-fraud strategy going forward. However, this will not provide complete protection against all fraudulent behaviour, highlighting the continued importance of prevention and detection measures provided by the Security - Fraud Risk and Analysis teams. PO now has the opportunity to build its own defences against fraud risk under a wider remit than at present; however fraud risk will need to be moved up the agenda for this to be realised.

Key issues

- No Exec owner to set the tone.
- No organisation wide policy or coordinated approach for management of financial crime.
- Effective mechanisms to prevent and detect fraud and corruption are not incorporated into policies, procedures and systems as standard.
- Risk of losing independent and specialist oversight of branch activity by Security – Fraud Analysis under Wave 3.
- Staff are not clear on where and how to report suspicions or concerns.
- No formalised process for detecting internal staff or agent remuneration fraud.
- Technology and tools to detect fraud are limited.
- A healthy dose of professional scepticism is not generally applied by staff when considering the potential for fraud.

Priority actions

- Formally nominate a GE member to be responsible for financial crime risk management.
- Identify financial crime risks organisation-wide and effectiveness of management.
- Determine the future state, commission a gap analysis and prioritise activities.
- Delegation of roles and responsibilities to deter, detect and respond to all fraud across PO.
- Moving management of fraud risk and more widely financial crime risk to one place.

POL00423307

Contents

POL00423307

Detailed Findings

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
1. Financial crime risk strategy, policies, procedures and guidelines						
1.1	**Anti-fraud policies, procedures**	There is no enterprise level or corporate policy for the management of fraud, or corresponding owner. This is likely to have contributed to the lack of clarity over management and staff responsibilities for ensuring that appropriate action is taken for preventing and detecting fraud. The impact observed has been the significant fragmentation of its management (particularly with regards to internal staff fraud).	Staff do not have a clear understanding over what part they play in the management of fraud risk. Organisational restructure / staff reductions may result in fewer internal controls such as segregation of duties, approval processes, supervision and rotation of staff. Tolerance levels for fraud and corruption are not defined.	**High**	a) Financial Crime Strategy / Policy should be developed and implemented. This should: • *have a GE owner to promote Board commitment.* • *Board approval.* • cover components: ***prevention, detection, deterrence and response.*** • roles and responsibilities clearly described. b) Relevant financial crime documents should be communicated. c) Effectiveness should be measured. This should be reported to ARC on an agreed basis.	Jane MacLeod **January 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
1.2	**Fraud Risk Management**	Whilst the Security team have built a fraud risk management framework covering the fundamental elements within the remit of their activity, it is focused on customers and branch facing activities (Network, Supply Chain and change projects). This does not currently cover: cyber, internal staff and supplier/partner, speak up (whistle blowing) and remuneration.	Financial, operation and reputational risk. Fraud goes undetected.	**High**	PO management of fraud risk and more widely financial crime risk should sit in one place.	Jane MacLeod **January 16**
1.3	**Policies, Procedures and Programmes**	When designing and implementing new systems, policies and procedures controls have not always been built-in to reduce the risk of fraud *(refer to detailed findings in Appendix 3)*. This is partly due to PO not fully understanding the high fraud risk areas. Whilst there is a Policy Review Group the Security - Fraud Risk team are not represented or requested for input to ensure 'fraud proofing' where relevant.	Staff are swayed by the opportunity (little fear or exposure or like hood of detection) to commit fraud. Investigation outcomes and fraud risk is not incorporated into policies and procedures.	**High**	a) Catalogue of policies and procedures should be assessed to identify which should be 'fraud proofed'. b) A risk based approach should be taken on the order of priority. c) Fraud proofing of policies and procedures should be incorporated into the remit of Policy Review Group.	Jane MacLeod John Scott **January 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
1.4	**Fraud Awareness Survey**	PO has not conducted a staff fraud awareness survey since separation to assess the level of understanding of anti-fraud policies, procedures and processes. Most organisations of similar size would do this as a matter of course.	Staff may not have the same level of understanding of PO's anti-fraud strategy.	**Low**	a) PO should undertake a fraud awareness survey of staff to assess their level of understanding of fraud related policies and procedures. b) Findings of the survey should be used to develop an action plan to address areas, where staff understanding of policies and procedures is not consistent. c) Such a survey should be conducted on a three yearly cycle.	Jane MacLeod **March 17**
2. Roles and responsibilities with respect to financial crime risk management (including cultural aspects).						
2.1	**Responsibility for Fraud Risk**	Whilst Security has taken on some of the mitigating fraud risk management activities, no function, team or individual has been formally delegated to act on behalf of Board or Audit and Risk Committee (ARC) to ensure that PO has appropriate arrangements to: deter, detect and respond to fraud.	Fraud risk management is low on the PO agenda. Sound ethical culture is not established. Lack of empowerment to inform and enforce policy.	**High**	a) Delegation of roles and responsibilities to deter, detect and respond to fraud across PO. This should cover as a minimum: • *Develop framework of anti-fraud policies and procedures across the business.* • *Raising awareness of fraud risks and developing mechanisms to maximise the opportunities for fraud risk reporting.*	Jane MacLeod ***a-c:*** **Jan 16** ***d:*** **July 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
					• *Responding to Speak Up and other concerns raised with management.* • *Investigation of suspicions and other irregularities.* • *Providing advice and recommendations to managers across PO on appropriate controls to help prevent and detect fraud.* • *Monitoring anti-fraud activity across PO.* • *Communicating of outcomes as appropriate.* b) Division of responsibilities should be defined across (as appropriate): General management; Risk and Compliance Committee; Audit and Risk Committee; CFO; HR; Security; ISAG; Legal; Mediation; Contract Advisors; Field Auditors; Internal Audit; Risk; External Audit; and Insurers. c) Clarified roles and responsibilities should be clearly communicated	

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
					organisation-wide. d) Provide RCC, ARC and wider GE with relevant training.	
2.2	**GE Ownership**	Direct responsibility for anti-fraud efforts does not currently reside with a member of GE. This lack of ownership has created significant challenges for Security, when attempting to prioritise the management of it. To exemplify, Security is reliant on the resources of Field Audit team within Network to complete visits on branches at risk. Due to Network Transformation priorities and resource limitations the monthly Field Audit visits have reduced from 50 (25 selected by Cash Management) to 30 (10 selected by Cash Management), whilst the risk exposure to PO given the change in suspension policy has increased.	Board tone over fraud risk management is not incorporated into working practices. Fraud risk management is not prioritised.	**High**	GE member to be responsible for coordinating financial crime risk management.	Jane MacLeod **Sept 15**
2.3	**Behaviour Framework**	Whilst PO has a clear Behaviour Framework acting with honesty and integrity is not a defined behaviour shaping the way we do things.	Culture at PO shapes itself. This may result in inappropriate behaviours.	**Medium**	Consideration should be given to the inclusion of honesty and integrity as defined behaviours within the Behaviour Framework.	Jane MacLeod **January 16**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
3. Reporting of suspicious activity and investigation processes.						
3.1	**Speak Up Policy, framework and high level processes**	*Roles and Responsibilities* The Risk team is responsible for the development and maintenance of the Speak Up Policy, framework and high level processes to support it. We noted that a framework has not yet been developed and staff awareness of high level processes has not been tested. There is also no formal link into the Head of Security or Security - Fraud Risk team (responsible for investigation of suspicions). However, there is a proposal to move the monitoring of the Speak Up (whistle blowing) line to Grapevine for business efficiency purposes. *Maintenance:* Whilst the Speak Up Policy has the fundamental elements, testing identified it was not up-to-date. The following concerns were raised with the Risk team and In touch (supplier): • the number within the Speak Up Policy was for RMG rather than PO. • whilst the number on the intranet was correct when tested the script used was for	Financial loss or exposure to regulatory or legal action. Ability to prevent a corporate crisis could be undermined. Staff do not report suspicions. Culture of silence.	**High**	Consideration should be given to the following opportunities relating to Speak Up: • *Having Speak Up Policy, framework / high level processes under remit of Security.* • *Speak Up Policy has a GE owner with published contact details.* • *Location of Policy on the intranet reviewed.* • *Speak Up contact methods are checked at agreed intervals.* • *Speak Up Policy is reviewed at least annually.* • *Policy applies to all i.e. employed in or working with PO.* • *Staff understanding is arrangements tested.* • *Speak Up arrangements are incorporated into training.* • *Intranet page for Speak Up should bring together various PO policies, procedures and codes relating to anti-fraud.*	Jane MacLeod **July 16**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		RMG. • the intranet page and Speak Up Policy offers an online web reporting service, however the link referred users to the RMG portal rather than PO. *Arrangements:* A review of arrangements identified the following areas for strengthening: • there is no overall named GE owner, including relevant contact details. • there is no formal training to support the Policy. • the location of the Policy is not overtly obvious on the intranet. • no suspicions of fraud have been reported via the hotline in the past 18 months. • the Policy does not apply to all i.e. employed in (staff and contractors) or working with PO (employees of suppliers).			• *Speak Up number is published on the intranet home page.*	
3.2	**Investigations**	PO has a clear investigations process in place when a suspicion or concern related to fraud is reported to Security. However feedback from staff has indicated a lack of consistency of response, if raised with and investigated by	Line managers may not have the necessary skills, experience or independence to undertake investigations to the required	**Medium**	a) An organisation-wide Investigation Policy (which includes a Fraud Response Plan) should be developed as a formal means of setting down clearly the arrangements for dealing with detected	Jane MacLeod **31 Jan 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		line management. Additionally management have highlighted confusion over who should conduct internal staff investigations and how this should be reported.	standards. This may result in loss or damage of evidence, abuse of process or failure of the investigation.		or suspected cases of fraud. b) Financial Crime and Speak Up policies should refer to the Investigation Policy. c) Investigation Policy should be linked to staff Code of Business Conduct. d) Investigation Policy should be owned. The document should be published via the intranet.	
4. Governance structures for overall monitoring and upwards reporting of financial crime activity and financial crime risk.						
4.1	**ARC responsibilities**	Whilst the Terms of Reference for the Audit and Risk Committee (ARC) refers to various responsibilities for managing the risk of fraud *(refer to Appendix 4)* it is not obvious these are formally being performed. We noted that: • fraud risk and more broadly, financial crime is not a standing agenda item. • the ARC does not receive any regular reporting in this respect. • Head of Security is not an attendee at ARC or Risk and Compliance Committee (RCC).	Inadequate anti-fraud programs and controls in place to identify potential fraud. Investigations are not undertaken when fraud is detected. Fraud is not prevented.	**High**	a) ARC should review its responsibilities to ensure it has sufficient oversight over the design, execution and monitoring of antifraud controls. b) Head of Security should be invited to attend the RCC and ARC when required (at least annually).	Jane MacLeod **31 Jan 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
5. Financial crime risk management (including appetite, identification, monitoring and awareness of financial crime risks).						
5.1	**Risk**	The Risk Register for Security includes areas within its remit where PO is susceptible to fraud. However PO does not fully understand its exposure to fraud risk more widely, due to the localised approach taken and therefore does not know whether it has the right range of mitigating controls in place.	PO does not effectively manage fraud risk.	**High**	a) A fraud risk assessment should be performed in all areas. b) PO regularly identifies and assesses fraud risks – perhaps as part of an overall risk management process.	Jane MacLeod **31 Jan 16**
6. Use of technology to detect financial crime.						
6.1	**Fraud identification process**	PO lacks enabling technology to robustly detect fraud at branches. The Security - Fraud Analysis team uses a number of data sources to produce weekly and monthly spread sheets (limited number) from which they identify a fixed number of branches of higher risk (due to the resource constraints of the Field Audit). These are assigned for further investigation. Part of this investigation includes use of a tool they have built called a 'fraud checker' that pulls on the reports. There are a number of inherent challenges and risks: • it does not update automatically or allow for real time queries.	Fraud remains undetected. Losses are not found consistently and quick enough. Significantly large losses impacting the bottom line. Judgemental error when analysing reports.	**High**	The need to move from Horizon to a new Front Office Application (FOA) provides an ideal opportunity to reassess the requirement for fraud detection tool.	John Scott **Immediate**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		• it requires significant human input, intervention and specialist knowledge (it takes one FTE a week to complete the initial analysis) i.e. it does not automatically flag branches requiring review. • does not include data upon which Sub Postmaster remuneration is based (circa £500m per annum). • there are instances of large losses occurring where the reports have not flagged the branches as high risk.				
6.2	**Front Office Security - Fraud Risk Team Impacts**	The move from Horizon to the Front Office Application (FOA) will have significant operational impacts for Security - Fraud Analysis team in terms of continuity of data provision used for interrogation. At the time of the review Security had not been invited to the FOA project workshops.	Significant resource impacts during transition leading to a reduction in the number of branches that can be reviewed for anomalous behaviour. Larger losses due to untimely audits.	**Medium**	a) Impacts on Security - Fraud Analysis team resource and business-as-usual activity during transition which should be considered by the project team. b) Risks associated with transition should be reflected within the Security Risk Register.	John Scott **Immediate**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
6.3	**Front Office – Design Requirements**	Security has documented detailed design requirements for the FOA which have been captured by the project team. Approximately, 80% of the requirements are either already in plan or will be included within the detailed requirements phase. This has been validated by the National Federation of Sub Postmasters. The most important requirement will be for Security - Fraud Analysis team to have direct access to all the FOA data.	Lessons learnt from Horizon are not incorporated into FOA.	**High**	a) Any proposed de-scoping of end-user requirements should be communicated to Head of Security. b) End user requirement for being able to directly access all FOA data for investigation purposes should be considered as mandatory.	John Scott **Immediate**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
7. Training and communication.						
7.1	**Anti-Fraud Culture**	Security uses various techniques to foster fraud awareness within Network, Supply Chain and change projects. Success is limited due to a lack of promotion by the business of its expectations over fraud risk management, behaviours etc.	Staff do not have a clear understanding over what part they play in the management of fraud risk or behaviours expected.	**Medium**	a) A financial crime awareness programme should be developed PO wide. This should include reminding relevant staff at least annually of their fraud risk responsibilities. b) Partners and suppliers should be reminded of their counter financial crime responsibilities and PO commitment to protect funds. c) Regular awareness messages concerning emerging fraud risks that affect PO and its staff should be publicised.	Jane MacLeod **31 Jan 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
7.2	**Training**	A training programme is developed on an annual basis within Security focusing on known areas of fraud weakness within Network and Supply Chain (particular focus of remit). Whilst the programme is signed off by the Head of Security, there is currently no input or endorsement from ARC, RCC or GE. Apart from the Annual Info Security Day conducted within branch there is no coordinated training activity that addresses fraud risk.	Staff who have a role in prevention and detection of fraud miss flags through lack of clarity over what constitutes fraud, how to identify such behaviour and how to respond if it is suspected.	**Medium**	a) Financial crime awareness training (including Speak Up Policy) should be covered during induction for new staff in all business areas. b) Consideration should be given for regular financial crime training for all staff being mandated by the Board.	Jane MacLeod **31 Jan 16**
8. Implementation of actions to reduce identified financial crime risks to acceptable levels.						
8.1	**Post Investigation Reviews**	Post Investigation Reviews (PIRs) are completed by the Security - Fraud Analysis team for any Network losses over £25K as a lessons learned exercise. Actions are proposed in response. PIRs are shared with various Security stakeholders. These are shared more widely for larger losses, however this is not formalised.	Sufficient action may not be taken more widely by the business (business-as-usual or policy changes). Large losses increase.	**Medium**	a) PIRs should be renamed / branded to avoid confusion with the Post Investment Review etc. b) Outputs should be shared with GE owner for fraud risk and formally reported to Risk and Compliance Committee (RCC).	Sally Smith **Immediate**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
8.2	**Products**	Prior to the new 'Change Process' the Security - Fraud Risk team Senior Manager attended the Project Delivery Governance Forum to ensure that fraud risk was considered when PO is designing, changing and implementing products. Under the current arrangements the Forum has been disbanded and replaced by Clearing House and Transformation Committee. Whilst the membership of these Groups is more senior to ensure robustness of challenge and elevate decision making, there are no formalised controls to ensure key stakeholders such as the Security - Fraud Risk team are duly consulted.	Project moves through its lifecycle which exposes PO to fraud risk outside of appetite or tolerance levels.	**Medium**	a) PO should be confident that controls are sufficient to ensure the right stakeholders are identified and adequately consulted. For example the change methodology could mandate a minimum set of stakeholders to be consulted which could be enforced / validated via gating processes. b) Security - Fraud Risk team should be viewed as a key stakeholder at Gating points.	Sally Smith supported by Change Management team **30 Oct 15**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
8.3	**Risk Assessment Tool**	A Risk Assessment Tool for projects has been proactively developed by Security - Fraud Risk team to determine the fraud risks to PO and level of team input required. To be effective this should be completed by the Project Manager after 'blue sky' thinking. There has been push back over the requirement to complete due to lack of endorsement by Clearing House. Recognising the need to still engage with the business the Security Fraud Risk Senior Manager continues to meet with the Portfolio Managers to establish the pipeline in the attempt to engage and build in controls. This is due to the diligence of the individual rather than a formalised and robust approach to assess fraud risk exposure of projects.	Products are developed which expose PO and SPMs to significant risk or exposure to fraud. Costs associated with cancelling a project or building in controls at a later stage. Impact on bottom line.	**Medium**	a) A formal risk assessment process should be established, reviewed and endorsed by Clearing House. b) Completion by Project Managers (prior to moving through Gate 1) should be mandated. c) Compliance should be monitored by the Transformation Committee.	Sally Smith supported by Change Management team **30 Oct 15**
8.4	**Supplier Management Information**	The Security - Fraud Risk team have faced challenges when requesting suppliers to share management information (MI) on significant fraud events, allowing PO to protect itself and agents against risk. This is partly due to PO not generally owning the product and contract	Losses that could have been prevented.	**Medium**	Agreed wording regarding the requirement of suppliers to report significant fraud events should be incorporated into the precedents at next review.	Sally Smith Next review of contract precedence.

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		obligations not mandating such information sharing. For example Money Gram has been subject to the biggest external fraud for PO. In 2014, 1K attempts were made (approximately £310K worth of losses). The fraud exposure was known to Money Gram, yet PO was not aware of this until Security - Fraud Risk team raised the losses with the supplier. The Security - Fraud Risk team has raised with Legal the need for wording to be included within PO contracts to ensure that suppliers make PO immediately aware of any significant fraudulent event that impact a particular product. Legal have agreed to include such wording within the next review of the contract precedence in 2015.				

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
9.1	**Making Good of SPM losses**	Prior to the Second Site review, unexplained losses at audit led to temporary suspension of the PM or SPM and in a significant number of instances this led to prosecution. This resulted in significant disruption and cost to the Network (i.e. using a temporary SPM). Against the backdrop of the Second Sight review and cost pressures this policy was changed. PO now investigates as far as possible without suspension. SPMs have the opportunity to "*make good*" the losses or missing monies "*with no prejudice wherever it has come from*". The nature of the loss is considered as opposed to the total sum. This involves a discussion been Field Support Adviser and Contracts team. The SPM also has the opportunity to settle centrally. Essentially, SPMs in the majority of cases are now being given a second chance to "*improve performance*". Whilst it is acknowledged that this move was strategic the new approach introduces a lack of clarity over whether such actions by SPMs are inherently dishonest or a direct result of	PO strategy may take precedence over ethical decision making. Dishonesty is not punished. Reputation damage. SPMs use PO money for interest free loans. Larger losses are not prevented.	**High**	a) PO needs to be clear when SPMs are making good losses, what is considered as: • *dishonest behaviour.* • *requiring performance improvement* b) A review of SPM's Business Case should be incorporated into PO decision making over whether behaviour is dishonest or requiring improvement.	Angela Van-Den-Bogerd **30 Nov 15**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		performance improvement needs.				
9.2	**Improving Performance**	The low number of further losses in those branches where SPMs have been allowed to make good has been viewed by the business as a success in improving performance. Seven repeat occurrences have been found as at May 2015. This is against a background of incomplete information being provided for analysis. The process for determining branch monitoring following the making good a loss was not in place at the time of the change in the policy. Consequently for the past year there has been no formalised focused monitoring of those branches (of higher risk) from a fraud or loss perspective.	Reputation damage from knowledge of SPMs being allowed to make good losses. Negative impact on SPM performance. Tensions between teams (Security, Contract Advisers and Field Audit) with competing priorities.	**High**	A full fraud check (developed by Security - Fraud Analysis) will be completed against a checklist to ensure consistency of those branches on a quarterly basis, until no longer required. Branches will also receive a visit by the Field Audit team roughly a year after non-suspension or reinstatement. Retrospective reviews have been scheduled over a period of time. A list of non-suspensions will be reviewed by the Security – Fraud Analysis team going forward. The change in policy on precautionary suspensions should be reviewed within the next 6 months against relevant metrics in order to assess whether it is deemed to be working.	Craig Tuthill **31 Jan 16**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
9.3	**Sparrow**	Sub-Postmasters (SPM) are continuing to cite errors in Horizon as the reason for losses. Interviews with the Investigations team highlighted that there is a continued reluctance to pursue such cases.	SPMs exploit POs perceived reluctance to pursue case linked to Horizon. Large losses impacting the bottom line. Morale of staff detecting and investigating fraud is damaged.	**High**	Whilst the lack of clarity over the response to such challenge was less clear over the past year, on closure of SPARROW and following the PO response to Second Sight the position going forward should be agreed and communicated (externally and internally).	Angela Van-Den-Bogerd **Immediate**
9.4	**Proceeds of Crime Bank Account**	Security is responsible for the Proceeds of Crime bank account. This does not form part of the PO automatic pooling process. The following issues (a result of an error in handover) were discussed with Security and Treasury: • the account had not been defunded for 18 months. As at March 2015 the account balances over £500k. • staff were not aware of the bank account existence due to those managing it leaving PO (error in handover). • three individuals named on the bank mandate had left PO without cancelling and transferring such	Withdrawals could be made which remain unidentified.	**Low**	The Security team have worked with Treasury to resolve the issues highlighted. The purpose of the account has been re-clarified including the process for defunding and £343k was been defunded during the audit. The chequebook has been cancelled and new signatories set up on the Bank Mandate. We are working with Treasury to ensure lessons learnt are built into processes going forward. A memo has been issued to the Treasury (outside of the review) which summarises concerns relating to bank	N/A

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		responsibilities. • the purpose of the bank account required re-clarification due to monies deposited into it not relating to the intended reasons for set up. • staff within Security were unaware of the requirement to defund the balance into the central profit / loss account. • the process of defunding was unclear. • the location of the cheque book was unknown.			accounts currently out of scope of Treasury. Areas for strengthening have been suggested relating to: maintenance of bank mandates, alignments of roles and responsibilities to PO Treasury Policy requirements, rationalisation of such accounts, defunding process and management of cheque books.	
9.5	**Prosecution Policy**	Prosecution Policy remains in draft since 2012. GC has recently taken ownership of it.	Lack of publicised deterrent.	**Medium**	Prosecution Policy is formally approved.	Jane MacLeod **30 Sept 15**

POL00423307

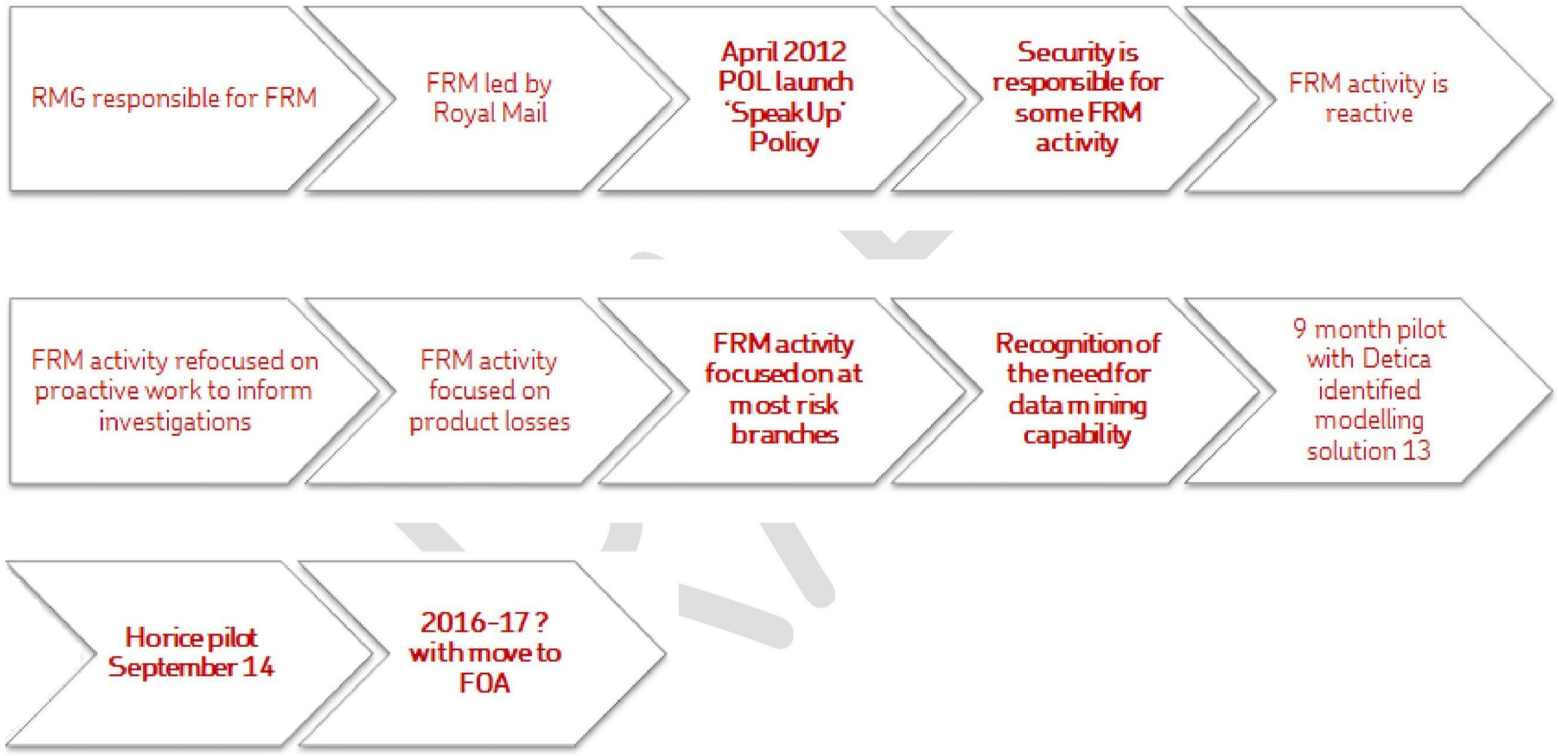
Appendix 1: Areas of Best Practice - Noted at Audit.

Area	Key areas of good practice
Strategy	• The Security team mitigating fraud risk management actions within remit. • Communication between Security - Fraud Risk, Cash Management, Field Audit and Contract Adviser teams. • Security liaison with external stakeholders re: fraud risk and investigations. • Significant reduction of excess cash (at risk) within the Network. • Joined up approach between teams across Security to ensure best outputs for PO / reducing overall fraud risk exposure.
Governance	• Head of Security attends Corporate Services Lead Team meetings. • Quality checking processes are incorporated into the Security - Fraud Analysis team processes. • Head of Security has a dotted reporting line into GC. • Security - Fraud Analysis team make the most of tools available to them to detect fraud within the Network. • On-going communication between Security - Fraud Analysis team and branches relating to non-conformance. • Security - Fraud Analysis team response to ad-hoc enquires by the business. • Formalised and documented processes for selecting branch for visits. • Specialist skills and experience of Security - Fraud Risk team.
Risk	• Action taken by Security to mitigate risks related to the Proceeds of Crime Account. • Response to identified PO and agent exposure to external fraud.
Awareness	• Security input into end user requirements of FOA. • Proactive efforts by Security - Fraud Risk team to raise fraud awareness within projects and incorporate robust controls to reduce exposure. • Communication and training on fraud risk within the Network.
Monitoring	• On-going review by Security - Fraud Analysis team over the effectiveness of reports (management information). • Updating procedures and flow charts to support processes. • Proactive efforts by Security - Fraud Risk team to develop and improve processes to drive fraud detection forward. • Monthly meetings to discuss case progress (investigators, Head of Security and Cartwright King with GC optional).

POL00423307

FINANCIAL CRIME

Appendix 2: Fraud Risk Management (FRM) – The Journey since Separation.



POL00423307

Appendix 3: Audited internal controls to assist in preventing and detecting financial crime.

The following areas were examined: ***recruitment screening, expenses (SAP and Capita), deductions, loans, annual leave, telecoms, corporate procurement cards (CPCs) and stock management***.

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
1. Recruitment						
1a	**Screening**	The Recruitment Policy states that PO applies a robust and a comprehensive approach to vetting and pre-employment checks. Whilst this is true for some categories such as CIT, Cash Centres (more traditional with access to physical cash), Directors, FS sales employees for all other roles (mainly in customer service centres), PO pre-employment checks for staff where there is no regulatory requirement are limited to: • *Criminal Records Bureau* • *Eligibility to work in UK* • *Proof of address* Security staff are subject to enhanced screening, however this is something instigated by team rather than Policy. Feedback from the HRSC Recruitment team suggests that reference and professional qualification checking are not viewed as a critical process. Whilst it is acknowledged that reference letters are a thing of the	PO appoints individuals who dishonestly claim to have professional qualifications or have not worked for previous employers. PO appoints individuals with lower levels of dishonesty into positions. PO will not be compliant for recruitment by FS regulated entities.	**High**	Reference checks and verification of qualifications should be dependent on the direct level of risk in the position an individual will occupy. Cost benefit analysis should be performed against the risk. The cost of changes should be shared with Al Cameron for consideration.	Neil Haywood / Joe Conner **30 Nov 15**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		past, performing a reference check from an outside source (such as telephoning a previous employer to confirm dates of employment, role title etc.) and verification of professional qualifications required for the role will help to ensure the best hiring decision is made by PO.				
2. Expenses						
2a	**SAP Travel Claims**	Staff continue to claim for travel expenses via SAP rather than using Capita. In addition to PO not getting best value from these travel bookings there are various fraud related concerns including: • staff are significantly exceeding the maximum limit agreed for overnight accommodation. • staff are claiming for the cost of travel or overnight accommodation when it appears to have been settled by Capita (this is being looked at outside the work to be reported). • Line Managers are approving such claims on SAP as appropriate.	Reputational risk in light of MPs expenses scandal. Staff use the travel receipt or invoice booked through Capita to claim a SAP expense. Wrong behaviours are encouraged. Impact to the bottom line.	**High**	a) Management should review the effectiveness of the Expenses Policy. This should incorporate 'fraud proofing' current arrangements. b) Management information should be shared with Cost Centre holders and the Cost Reduction Group regarding staff expenses via SAP and Capita for analysis and to inform future policy. c) When travel is not booked through Capita the following should be completed: • Line Manager should be ensuring adequate justification exists and is in accordance with the Expenses Policy. • Capita travel data should be sample checked	**TBC**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
					against SAP expenses to ensure the claim has not been duplicated.	
2b	**Reconciliation between claim and receipt**	Expenses claimed via SAP are subject to sample checking. Whilst the HRSC on a sample basis reconcile claims to receipts, we observed there is limited challenge over the appropriateness. We acknowledge the difficulties for the HRSC in doing this, given the lack of visibility over the individuals work. The Line Manager is therefore responsible for performing the appropriateness check; however they do not have visibility of staff receipts when approving the expense for robustness.	Inappropriate claims may be processed through SAP in the absence of an effective check on receipts. HRSC does not have all the information required to provide an effective check on the validity and appropriateness of the claim.	**High**	a) Managers should be reminded of their accountability for approving all expenses relevant to their cost centre. b) Guidance should be issued to staff regarding the approval of expense claims. c) Security - Fraud Risk team should include staff expenses and Capita travel data within remit of detective activities.	**TBC**
2c	**Capita Travel Requests**	Unlike expenses claimed via SAP staff do not require approval for Capita travel requests, so long as they are within the limits set out in the Expenses Policy. There is no link between SAP and Capita travel systems. Staff have the ability to: • select any notifer (i.e. does not require approval by Line Manager) irrespective of grade or function. • purchase season and multiple	Inappropriate Capita travel requests remain unidentified by Line Manager. Duplicate claims are made through SAP using the Capita invoice / rail ticket etc.	**High**	a) Comprehensive analysis should be performed of staff use of Capita for travel, identifying improvements based on: • Cost • Benefits • Risks b) Consideration should be given to restricting booking certain items via Capita: • blocks 10 anytime tickets. • first class tickets.	**TBC**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		tickets (block of 10 anytime tickets for some staff). • assign the expense to any cost centre. • duplicate a claim through SAP and Capita.			• monthly and annual rail season tickets. c) Exceptions should be approved by HR Business Partner.	
2d	**Contractual entitlements**	Individual contracts vary significantly in terms of staff entitlement. For example on staff travel reimbursement such as: *excess travel, transport costs from home to place of work, use of lease car and accommodation*. We noted that claims made by staff are not being checked against contractual entitlement. Furthermore the records held by the HRSC listing home, dualist, field and office based staff also appear to be out of date when reconciled against the claims made by a number of staff in 2014/15.	HMRC associated issues. Inappropriate claims are made which remain unidentified.	**Medium**	a) Line Managers should understand they have the responsibility for asking HR to re-issue contracts of employment if necessary, and that Line Managers are responsible for authorising payments to staff only if these are in accordance with their contracts of employment and/or in accordance with collective agreements reached with representatives. b) A policy statement on contract of employment should be reviewed, amended and reissued. c) Guidance should be given to managers about what they should be asking and checking before they sign off travel expenses to make sure this is rooted in agreed terms and conditions.	Colin Stretch **31 Dec 15**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
					d) HR to review staff place of work (with the respective contract) against the following categories: *Home, Dualist, Office and Field based.* This review should be repeated at agreed intervals.	
3. Annual Leave						
3a	**Entitlement**	There are no automated checks to ensure annual leave entitlements as set out in staff contracts are being applied in practice for employees (i.e. parameters are not set within SAP to ensure that annual leave balances are not exceeded by staff).	Staff take excess annual leave. Red flags (fraud indicators) may also not be visible such as staff refusing to take holidays.	**Medium**	Benefits and limitations (including costs) for enhancing SAP to incorporate parameters and automated checks for annual leave entitlement should be explored.	Joe Connor **Immediate**
3b	**Use of SAP**	The Annual Leave Policy does not mandate the use of SAP (for those with access) to request or approve annual leave entitlement. This has resulted in inconsistent, localised, offline procedures being adopted by staff.	PO is unable to test for fraud relating to annual leave.	**Medium**	Where staff have access, it should be mandated that they request and approve annual leave on SAP. Policy statement should be reviewed, amended and reissued.	**Colin Stretch 31 Dec 15**
4. Telecoms						
4a	**Acceptable Use Policy**	Whilst PO has an Acceptable Use Policy covering mobile phones this is limited	Telephony is open to	**Medium**	A corporate policy in support of the use of mobile phones	TBC

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		in terms of providing clear guidelines over user responsibilities, issuing, recirculation of devices, and reimbursement of personal calls.	misuse. Employees are unaware of the terms and conditions for mobile phone use.		should be developed. This should be aligned with the Acceptable Use Policy. As a minimum it should cover: • *Eligibility for a mobile phone.* • *Use of devices.* • *Exchange.* • *Confidentiality.* • *Leavers.* • *Reimbursement for personal calls.* • *Recirculation of devices.* • *Upgrades.* • *Loss.* • *Timetable for review.*	
4b	**Monitoring of usage**	The responsibility for monitoring appropriateness of telecoms usage has not been formally delegated. We observed that monitoring is limited to the top 10 highest users. Cost Centre holders are not currently provided with sufficient information on billing to enable such review. Our review of charges for the past 6 months highlighted 17 instances where staff have bills for over £500 per month (including 4 instances over £1k).	Telecoms are open to misuse by users.	**Medium**	Itemised bills for mobiles should be made available for review (Cost Centre holders/ Line Mangers) on a periodic basis.	TBC
4c	**Reimbursement of Personal Calls**	Consistent procedures are not being followed for the reimbursement of personal calls on PO mobile phones. The observed reasons for this include: • Azzuri (RMG legacy online billing and	PO is paying for a significant amount of personal calls (at least 25%).	**Medium**	a) Clarity is required over accountability for Azzuri contract. b) The effectiveness of Azzuri should be evaluated:	TBC

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		reporting supplier) receives a report of new users weekly, however email addresses are often missing or do not match the user name. • Azzuri sends two reminder emails quarterly (regarding staff reimbursing PO for personal calls). 18% of users have not responded in the past 6 months (longest period 5 years) which suggests that limited further chasing or action is taken by PO internally. • Azzui does not have the email addresses of users for 249 handsets. The user is unknown for a further 9 handsets.	User list is not fully known.		• resolve the mobile phone billing, reporting. reimbursement issues. • Resolve the gaps in user data. Minimum data requirements to be shared with Azzuri should be agreed and implemented. • At a minimum PO should provide Azzuri with urgency the following: *Telephone number* *User name* *Email address* • All users should be set up on PCM with an agreed deadline. A KPI should be agreed with Azzuri to ensure timeliness of this going forward. c) Management (Cost Centre holders or Line Managers) should ensure reimbursement of personal call charges for mobile phones have been followed up consistently in their departments.	
4d	**Leavers**	A reconciliation between the 'Outstanding for Reimbursement' report (March 2015) provided by	PO is paying for call charges incurred by non-employees.	**Medium**	a) Handset portfolio should be reviewed. b) Each handset should have	**TBC**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
		Azzuri and leavers list (since April 2014) found the following: • nine leavers with active numbers being chased to reconcile (dating back to July 2014). • six leavers with active numbers who appear to have used their mobiles after termination date with 4 currently using the numbers. • one leaver (included above) who left PO in July 2014 has two active numbers, one of which incurred a bill in March 2015. Whilst the amounts involved are small the findings could indicate a wider issue relating to management of the handset portfolio. The total amount incurred overtime could prove significant. **The exceptions were raised immediately to Procurement who manages the providers.*	Azzuri chase individuals to reconcile call charges who no longer work for PO.		an assigned user who is a current employee. c) Active numbers assigned to individuals who have left PO should be cancelled immediately.	
5. Corporate Procurement Cards						
5a	**Payments**	CPC payments are automatically debited centrally on a monthly basis. We identified that payment processes are not subject to reconciliation to ensure the appropriateness of spend. A walkthrough of processes also highlighted that transactions are not subject to <u>any</u> review in a significant number of instances (i.e. neither by Line Manager nor cardholder when statements are not received).	Staff are tempted to inappropriately use the CPC facility. This remains undetected by PO. Sophisticated and high-level fraud. Purchases of items intended for personal use,	**High**	a) A policy decision should be made over the use of CPCs. b) PO should review and increase the level of scrutiny and controls applied to CPC transactions. This should include: • CPC policy and guidance updated to specifically mention the requirement	**TBC**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
			duplicate items, and unusual patterns remain identified.		for defined management checking processes for usage. • Further clarity is required on the line role. • Sample compliance checking should be built into processes.	
5b	**Review of CPC Statements**	Testing revealed that cardholders are not receiving statements in a significant number of instances to confirm that expenditure incurred is accurate.	Suspicious activity or errors remain unidentified. Incorrect statements could be paid.	**Medium**	Cardholders should be requested by the CPC Administrator to confirm whether or not statements are being received. * *Also refer to recommendation 5c below re loading and reconciling of transactions in SAP.*	Lorraine Garvey / Kate Wilson **31 Oct 15**
5c	**CPC Policy and guidance**	The CPC policy and guidance does not offer any clarity over who should approve expenditure and what this means. There is currently no further approval of CPC expenditure by management after the initial approval of card.	Lack of tone at top to prevent inappropriate behaviours.	**Medium**	Line Manager approval of spend should be introduced to ensure appropriateness of CPC expenditure. The following options should be considered: • Explore the possibility of the CPC provider (HSBC) providing an electronic download of transactions, which can be loaded into SAP and reconciled / approved by Line Manager through staff expenses (**Considered**). • Line Managers should review	Lorraine Garvey / Kate Wilson **30 Nov 15**

POL00423307

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
					statements on a monthly basis (if above is not possible). Sample checking should be performed to ensure compliance. • Alternatively statements are no longer paid centrally instead by the cardholder and claimed back through expenses.	
5d	**Allocation of costs**	CPC purchases are automatically allocated to relevant cost centres.	CPC transactions have been miscoded when individual has moved roles without notifying the CPC Administrator.	**Medium**	a) A review of the cardholders should be performed to ensure that individuals have not transferred position / assigned the right cost centre. b) CPC Administrator should be notified when a cardholder moves roles.	Lorraine Garvey / Kate Wilson **30 Nov 15**
6. Stock Management						
6a	**Inappropriate Sale**	PO stock is being sold by staff and agents on auction websites such as EBay (in some instances after being reported as destroyed). There is no dedicated resource currently to address this issue.	Fines from third parties. Individual imitating as PO. Brand reputation	**Medium**	Define the appetite for protecting the brand against resale of stock by staff online. More widely PO should consider the need for the following: • *Brand Protection Strategy*	Jane MacLeod *to raise with Pete Markey* **30 Nov 15**

POL00423307

FINANCIAL CRIME

Ref	Area Reviewed	Findings	Risk	Priority	Proposed Action	Owner/Date
			damage.		• *Brand Protection Programme* • *Dedicated resource*	

POL00423307

Appendix 4: Audit and Risk Committee Terms of Reference

- Significant findings (the "management letter" from external auditors) and recommendations together with management's responses.
- Any reportable restrictions experienced regarding scope or access to required information by either external or internal audit.

4.3 Fraud, Theft and Ethics

The Committee will

- Review with management their fraud assessment, detection measures and their investigation of illegal acts, as appropriate.
- Review any summary of frauds, thefts and other irregularities of any size.
- Review with the internal auditors and the external auditors the results of any review of the compliance with the Company's codes of ethical conduct and similar policies including whistleblowing.

4.4 Risk Management – Other

- The Committee shall have the power to conduct or authorise investigations into any company matters within the Committee's scope of responsibilities. The Committee shall be empowered to obtain independentlegal advice, and engage counsel, accountants, or others to assist it in the conduct of any investigation.
- The Committee shall perform such other functions as may be assigned or delegated to it by the Board, and may review other items of an internal control or risk management nature which may from time to time be brought before the Committee.