POL00423568

Risk and Compliance Committee Agenda

Date:	Thursday 4 July 2019	Time:	13.00 – 16.10	Location:	2.18 Norwich

Present:	Other Attendees:	
• Alisdair Cameron (Chair) • Cathy Mayor (deputising for Debbie Smith) • Chrysanthy Pispinis (deputising for Owen Woodley) • Mo Kang (Group HR Director) • Rob Houghton (Group Chief Operating Officer)	• Ben Foat (General Counsel) • Johann Appel (Head of Internal Audit) • Jenny Ellwood – by telephone (Risk Director) • Jonathan Hill (Compliance Director) • David Parry (Senior Assistant Company Secretary) • Mark Fabes (item 3) (Interim Group CIO) • Tony Jowett (item 4) (Chief Information Security Officer)	• David Mann (item 4) (Head of Information Security & Supplier Risk) • Ben Cooke (item 5) (IT Director – Back Office) • Barbara Brannon (item 7) (Purchasing Director) • Tim Armit (item 8) (Business Continuity Manager) • Mark Dixon (item 11 (Head of Tax & Treasury) • Andy Bear (item 11) (Account Manager, Locktons) • James Scutt (item 9.3) (HO Customer Experience Strategy & Deploy)
Apologies: Debbie Smith; Owen Woodley		

Agenda Item		Action Needed	Lead	Timings
1.	**Welcome and Conflicts of Interest**	Noting	Chair	13.00 – 13.05 (5 minutes)
2.	**Minutes and Action Lists**	Approval		
3.	**PCI-DSS Update**	Noting	Rob Houghton/Mark Fabes	13.05 – 13.15 (10 minutes)
4.	**Security Strategy** includes • discussion on Cyber Risk Appetite	Noting & Input *Onward submission to the ARC.* Noting	Rob Houghton/ Tony Jowett/ Jenny Ellwood/ David Mann	13.15 – 13.30 (15 minutes)
5.	IRRELEVANT **Back Office Transformation Update**	Noting & Input	Ben Cooke	13.30 – 13.45 (15 minutes)
6.	**Combined Risk, Compliance and Audit Update paper,** includes: • Consolidated departmental reports • Due diligence on multiples	Noting & Input *Onward submission to the ARC.*	Jenny Ellwood/ Jonathan Hill/ Johann Appel	13.45 – 14.45 (60 minutes)
7.	**Supplier Contracts out of Governance**	Noting & Input	Barbara Brannon	14.45 – 14.55 (10 minutes)
8.	**Business Continuity Update and Policy**	Noting & Input	Tim Armit	14.55 – 15.10 (15 minutes)
9.	**Policies**			
9.1	Anti-Bribery and Corruption Review and Policy (including Gifts and Hospitality)	Approval	Jonathan Hill	15.10 – 15.20 (10 minutes)
9.2	Whistleblowing Review and Policy	Approval	Jonathan Hill	15.20 – 15.30

Strictly Confidential

POL00423568

Risk and Compliance Committee Agenda

				(10 minutes)
9.3	Modern Slavery	Approval	James Scutt	15.30 – 15.40 (10 minutes)
10.	**GDPR Update**	Noting & Input	Jonathan Hill	15.40 – 15.50 (10 minutes)
11.	**Corporate Insurance Renewal**	Noting & Input	Mark Dixon/Andy Bear	15.50 – 16.05 (15 minutes)
12.	**Review of draft Audit, Risk and Compliance Committee meeting agenda** Note: An additional ARC meeting is being organised for w/c 22 July to approve the PwC Audit and ARA Note: The next ordinary ARC meeting will be held on 29 July 2019	Discussion	Chair	16.05 – 16.10 (5 minutes)
12.	**Any other Business** Note: The next ordinary RCC meeting will be held on 3 September 2019.	Discussion	All	

POL00423568

2

POST OFFICE LIMITED RISK AND COMPLIANCE COMMITTEE
Minutes of a Risk and Compliance ("RCC") meeting held at
Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ
on 9 May 2019 at 13.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Interim Chief Executive Officer
	Priyanka Dewan (PD) (on behalf of Owen Woodley)	Senior Strategy Manager
	Ben Foat (BF)	Legal Director
	Rob Houghton	Group Chief Information Officer
	Mo Kang	Group HR Director
	Cathy Mayor (CM) (on behalf of Debbie Smith)	Finance Director, Retail
In Attendance:	Veronica Branton (VB)	Head of Secretariat
	David Parry (DP)	Senior Assistant Company Secretary
	Johann Appel (JA)	Head of Internal Audit
	Jenny Ellwood (JE)	Risk Director
	Jonathan Hill (JH)	Compliance Director
	Liz Robson (LR)	CIO – Retail (item 3.)
	Deana Herley (DH)	Senior Manager, Assurance (item 5.3)
Apologies	Debbie Smith, Chief Executive Officer, Retail, Owen Woodley, Chief Executive Officer, Financial Services, Telecoms and Identity, Group Marketing and Group Digital & Innovation.	

1. Welcome and Conflicts of Interest **Actions**

Following introductions round the table, Alisdair Cameron opened the meeting. He remarked that the pack needed to be streamlined and that papers should be condensed, identifying the most significant risks and issues, what we were going to do to address these and the timeframes for doing so.

2. Minutes and Action Lists

The minutes of the RCC meeting held 14 March 2019 were **APPROVED.** Progress on completion of actions as shown on the action log were **NOTED.**

3. PCI-DSS Update

Liz Robson provided a verbal update on PCI compliance.

She explained this update would focus on the progress made on the alternative approach to banking services under investigation which would result in these transactions not being processed through Horizon and therefore not being in scope for PCI compliance. The progress report requested by ARC had been circulated for noting.

Regarding retail transactions via pin pad devices in branch, the deployment of point-to-point encryption (P2PE) of the Pin-Pad estate remained on track to plan, with devices being shipped to enable the required software upgrade and physical swap-out in branch.

PCI accreditation linked to the pin pad devices expired in the next 12 months and steps had been taken with Global Payments (our acquirer) to extend this accreditation until 2023 following accreditation testing. Accreditation cover came with the proviso that no further software changes would be made to the pin-pad devices beyond P2PE. An update from the Branch Device and Strategy Review on the future

POL00423568

of Pin-Pad device for branches, along with other devices such as Paystations, was expected at the end of May.

Regarding banking transactions, positive progression had been made with Ingencio and Vocalink to process transactions directly with the banks via the Ingencio cloud. This approach removed the POL back-end from PCI scope, helping to simplify the process of achieving PCI compliance by moving these transactions out of scope. Design and planning sessions were in train with payment partners and a revised timeline plan plus associated costs was expected at the end of May 2019. P2PE deployment would not be impacted and remained crucial for PCI compliance being achieved. Work remained ongoing in parallel.

The recent Data Audit of the systems estate was almost complete, with low instances or no instances of PCI related data being identified. PCI data that had been identified was removed and users educated to prevent further occurrences. Audits for Computacenter and Accenture remained outstanding and completion dates would be confirmed with both partners.

The team had remained actively engaged with Nettitude, our Quality Security Assessor (QSA) and Global Payments throughout this activity, and our Acquirer was also fully aware and supportive of our plans. A full plan update would be provided at the end of May 2019.

A number of points were raised:

What challenges were associated with data encryption for banking transactions, as an alternative to processing data through Horizon? It was reported that there were two main challenges: 1) reconciliations and 2) banks needing to change their systems. A workshop was taking place with Ingenico and Global Pay to assess the technical feasibility of an alternative approach.

The timescale for achieving PCI Compliance. It was reported that we would not be PCI compliant by the end of the year and JE and LR were working on identifying the associated risks, including the views of our partners.

The following was **AGREED:**

1. The Data Audit paper would include a section on how a BAU process would be implemented to monitor/scan the systems estate to identify and action any appropriate remediation for any PCI-related data. **LR**
2. The Branch Device Strategy paper would include an assessment of requirements of pin-pad devices in the future if they were going to be used for data entry by customers. **LR**
3. Mark Siviter would provide an update on current negotiations with RMG on the solution for International Data Capture.

A holistic plan on achieving PCI compliance, our position on data security and management (structured and unstructured data) and our risk controls would be presented to ARC in May.

4. Internal Audit (IA)

4.1 Internal Audit Report (IAR)

Johann Appel reported that apart from two change reviews, which had been deferred as part of the re-prioritisation plan, the Audit plan for 2018/2019 had been completed. 17 reports had been finalised with seven cleared by management. There was no outstanding fieldwork required for completion, and at 30 April 2019, there were no overdue actions.

AC requested that JA pass on his thanks to the team.

The RCC discussed the contents of the reports and noted that whilst there were no significant areas for concern, the message(s) conveyed could be more clearly identified. It was felt the reports should be focussed so that ARC members were fully aware of the key risks, the expected impacts, whether there **To do: JA**

POL00423568

were any shortcomings and the mitigating actions. Where appropriate, reports should be benchmarked against other industries and we should indicate where lessons from one report could be applied to other parts of the business.

It was suggested that the Internal Audit Report on Cyber Security needed to bring out the extent of our vulnerability, how long it would take to reach an acceptable position with reference to industry benchmarks, the prime drivers of weaknesses (e.g. not having strong passwords) and the activities we were undertaking such as tightening of controls around critical data assets.

It was noted that the security issues with some Payzone devices was not within the scope of the audit but Jenny Ellwood would reference this in her risk report.

JA was asked whether he had any concerns in relation to future audit reports planned or any other issues he wished to flag. He reported that terms of reference have not been agreed with process owners yet. The ToRs were in place for the Pensions Internal Audit. The Telco Internal Audit was at an early stage of planning. JA and RH would discuss the proposed change assurance work for the payment technology programme.

The reports would be circulated to the ARC for noting.

5. Risk

5.1 Consolidated Risk Report

Jenny Ellwood presented the consolidated risk report.

She reported that PCI, Information Security, Litigation and Change workforce remained the key risks but that there had been positive progress in relation to Information Security, including piloting some testing of third party supplier information security arrangements.

Emerging risks included uncertainty around the stability of the Government; people risk because of measures in the pipeline such as the introduction of a redundancy cap and because there had been significant people changes in critical roles recently and further organisational design changes were planned; and, the risk of the regulator taking action to address loyal customers' potential disadvantage vis-à-vis new customers. It was suggested that we should include what our mitigating actions would be in response to the loyalty super complaint.

It was **AGREED** that we would:

- Check whether RMG was affected by LINK ceasing to settle for partner banks from 1 July 2019.
- Include an update on the Fit and Proper compliance risk.

5.2 Litigation Update

The second trial relating to the Horizon system was pending direction from the Court of Appeal following our application to recuse the managing judge, which had been denied. The trial was due to resume on 4 June 2019 until early July.

5.3 Annual Report and Accounts 2018/19 – key risks

Deana Hurley presented the Risk Report for the Annual Report and Accounts 2018/19.

The principal risks and top risks were noted.

DH commented that since the publication of the last Risk Report there had been two main changes. Firstly the risk of increased likelihood of litigation had been amended from unlikely to possible, and

POL00423568

secondly, the risk related to Technology and Business Interruption had increased in impact as a result of being unable to automatically failover the second datacentre.

AC requested a review of the wording of the report. RH remarked that the cyber security risk had reduced as control effectiveness had improved; we were still not within risk appetite but we would be providing more information on additional risk mitigations.

The Executive Declarations were noted. The following was **AGREED**: **DH**

- Mitigating actions should be included.
- The GLO litigation should be included under the risk section and should be expanded to include details of the risk(s) involved, timings, costs involved (where available) and any operational changes that may be required.
- Health and Safety had not previously been included as a risk but should be referred to.

An updated paper would be presented to ARC in May.

6. Compliance

6.1 Compliance Report

Jonathan Hill presented the consolidated compliance report.

The following key points were noted.

Ofcom would investigate the text relay breach and assistance was being provided to respond to information requests from Ofcom. Difficulty had arisen in that Ofcom wished to understand the position dating back to 2002. JH believed the potential penalty was likely to be hundreds of thousands of pounds, but it was noted that the self-declaration and wish to settle early had been well received by the regulator and was likely be taken into consideration. The regulator had also recognised the mitigating actions we had completed to date.

6.2 Fit and Proper: Compliance with HMRC June 2019 Deadline

Since the last RCC meeting, the project team had focused on completing fit and proper returns. A large backlog of responses had been cleared and HMRC had agreed to extend the June 2019 deadline to September 2019 for MI data gathering purposes.

The RCC noted the improved and accelerated position but requested that the risks and how they would be tracked were identified. To do: **JH**

HMRC had increased branch registration fees from £130 per annum to £300 per annum from 1 May 2019. Fees would be in the region of £1.3 million and the plan was to stagger payments. Around 4,000 registered branches processed a limited number of transactions. Work was being undertaken on the implications of not providing a Forex service in those locations; however it was not thought that we should remove the service during the course of the litigation except where there were no transactions in a branch.

Appointed Representatives

Work remained ongoing with CAP ONE on the Appointed Representative appointment. Any new arrangement would need to be consistent with the current approach taken with our existing regulatory principals.

Approved person forms would need to be filed at Companies House once completed.

Vulnerable Customers' Policy

POL00423568

An external assessor had provided positive feedback on our vulnerable customers' policy and the associated training in branches.

Whistleblowing Policy
A question was raised about whether our whistleblowing policy was being used as we would hope. JH advised the whistleblowing hotline would become a Freephone number and that work was being undertaken by HR to encourage a culture which encouraged employees to raise issues of concern.

7. Cyber Security

RH advised that the main update of note was the work that had taken place on penetration testing of Payzone devices and the work now underway with the IT Security team to formulate a risk treatment plan to remediate vulnerabilities identified.

8. Business Continuity Plan and Policy

The paper and policy were **NOTED** but the item was deferred.

The POL policy template needed to be used and the risks and mitigating actions need to be clearer.

It was **AGREED** that with assistance from RH and JH, an updated paper and policy would be presented to the RCC and ARC in July 2019. **TA/RH/JH**

9. GDPR Update

The paper was **NOTED**.

AC felt that the paper should use less technical language and be simplified to bring out the key challenges and the next steps. We also needed to provide a complete picture of data and not just the personal data covered by GDPR to provide the ARC with a holistic view. Further work required on data should also be set out.

The RCC noted that some contract remediation was outstanding and that before the GDPR programme could be signed off, the transition from programme to BAU needed to be clarified. It was also proposed that privacy/GDPR champions should be established group wide.

It was **AGREED** that:

1. A revised paper would be presented to ARC showing the work completed to date, and the areas of outstanding work. **JH**
2. An Internal Audit would be completed in Spring 2020. **JA**

10. Review of draft Audit, Risk and Compliance Committee meeting agenda

The draft ARC agenda for 29 May 2019 was **NOTED** and discussed.

A consolidated report for Risk, Compliance and Internal Audit would be presented to ARC.

11. Any other Business

11.1 Meeting dates

It was noted that the next scheduled RCC meeting was on 4 July 2019.

POL00423568

Post Office Limited Risk and Compliance Committee Actions
Updated: 26.06.19

REFERENCE	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN/CLOSED
RCC Meeting 09.05.19					
3. PCI-DSS					
	Data Audit paper: The Data Audit paper would include a section on how a BAU process would be implemented to monitor/scan the systems estate to identify and action any appropriate remediation for any PCI-related data.	Liz Robson	July 2019	Ben Cooke: The PCI Program team have already scanned our vendor estates taken remedial action. They are working through the future operating model, which will include setting up regular scanning with our vendors.	
	Branch Device Strategy paper: The Branch Device Strategy paper would include an assessment of requirements of pin-pad devices in the future if they were going to be used for data entry by customers.	Liz Robson	July 2019	Michael Austin: In hand. But to set expectations, I have not seen any requirement for data entry over and above energy payments related to paystation which are being replaced by ICT 250s this year and with PZ Gen 3 devices over the subsequent 2 years or so. Both of these support data entry through App upgrades. So if pin pads = PED (i.e. payment terminal) then there is no view on changing these until FY 22/23 and maybe as late as 24/25. This replacement will be largely driven by a payment strategy and any P2PE related stuff with Ingenico.	

POL00423568

Post Office Limited Risk and Compliance Committee Action Log
Updated: 14.02.19

	Mark Siviter would provide an update on current negotiations with RMG on the solution for International Data Capture.	Liz Robson	July 2019	Update to follow from Mark Siviter.	
	PCI Compliance: A holistic plan on achieving PCI compliance, our position on data security and management (structured and unstructured data) and our risk controls would be presented to ARC in May.	Liz Robson	May 2019	Presented to ARC in May.	Closed
5. Risk					
5.3 Annual Report and Accounts 2018/2019 – key risks	• Mitigating actions should be included. • The GLO litigation should be included under the risk section and should be expanded to include details of the risk(s) involved, timings, costs involved (where available) and any operational changes that may be required. • Health and Safety had not previously been included as a risk but should be referred to. An updated paper would be presented to ARC in May.	Deana Hurley	May 2019	Presented to ARC in May.	Closed
8. Business Continuity Plan and Policy					
	It was **AGREED** that with assistance from RH and JH, an updated paper and policy would be presented to the RCC and ARC in July 2019.	Tim Armit	July 2019	In July's RCC agenda.	Closed
9. GDPR Update					
9.	1. A revised paper would be presented to ARC showing the work completed to date, and the areas of outstanding work.	Jonathan Hill	July 2019	Presented to ARC in May	Closed

POL00423568

Post Office Limited Risk and Compliance Committee Action Log
Updated: 14.02.19

9.	2. An Internal Audit would be completed in Spring 2020.	Johann Appel	Spring 2020		

Strictly Confidential

POL00423568

POST OFFICE
RISK AND COMPLIANCE COMMITTEE

Noting

3

PCI Compliance Status Update

Author: Phey Rasulian
Sponsor: Rob Houghton
Date: 28th June 2019

Executive Summary

Context

The PCI Programme issued an update to RCC on the 17th May 2019, this paper provides a progress update, specifically progress made with the improved approach to the banking and retail transactions processing capability, the progress of the Point-to-Point Encryption (P2PE) deployment across the pin-pad estate and the overall plan timeline to achieve full PCI compliance.

Questions this paper addresses

1. What is the progress of the technical solution to simplify processing of banking and retail transactions from the pin-pad?
2. What other routes technical/commercial are being explored to improve Post Office's PCI stance?
3. The outcome of the data audit?
4. How will we change our operating model to ensure process/procedures are in place to maintain PCI compliance?
5. What is the overall timeline for achieving full PCI compliance, including progress of the Point-to-Point Encryption (P2PE) deployment?

Conclusion

1. VocaLink and Fujitsu have provided resources to commence design activities; however, Ingenico has stated that they do not have the right individuals available until late August/early September this has resulted in an escalation into their senior executive team to explore reordering their priorities. Multiple communications have been exchanged to progress the situation, and Ingenico has reassured Post Office that this is a high priority.
   In parallel Post Office are exploring two other routes to improve Post Office's PCI compliance stance: The applicability of PCI regulation to banking transactions and the possibility of engaging alternative partners to compliment or replace Ingenico should the need arise.
2. The data audit is complete. The low number of occurrences were found and will be remediated by the programme either by removal or storage in accordance with PCI regulations. A schedule and scope of ongoing scanning will be developed to identify
3. Our continuing operating model improvements identified multiple products and processes that need assessing as to their PCI compliance. The identified items are being analysed, and a plan will be formulated to remediate the ones that are non-compliant.

POL00423568

4. Due to the lack of engagement from Ingenico, this has delayed the detailed design planning, and subsequently to improve the ability to forecast date for completion. The current plan continues to show 2Q/2020 to 4Q/2020. Once a delivery commitment has been received from Ingenico, the forecast will be revised.

Current status

2 Point-to-Point Encryption (P2PE) & Banking Transaction Processing Solution

2.1 Point-to-Point Encryption (P2PE) at the point of entry into our estate: the pin-pad devices in branch. The rollout of P2PE enabled pin pads is underway with the agreed plan for collection, shipment, firmware upgrade and in-branch device swap-out. The pilot is scheduled for the end of August, and if proven successful, the full rollout will commence the beginning of September.

2.2 The joint solution with Ingenico, Vocalink (Santander/POca), Global Payments and Fujitsu has stalled due to the delay of Ingenico's engagement. Whilst the escalation is being progressed with Ingenico; the programme team are exploring secondary technical and commercial/regulatory options to overcome the potential delay.

2.2.1.1 Technical options: Exploring if Global Payments can process the banking transactions rather than Ingenico, therefore, lessening the reliance on Ingenico and shifting it to Global Payments, subject to the resultant conversation this may be a quicker route to resolution.

2.2.1.2 Commercial/Regulatory options: Exploring if banking transactions can be excluded from PCI-DSS regulation. The Post Office legal and banking team have engaged external lawyers CMS and Payment Service Regulator (PSR) respectively to seek guidance on the applicability of PCI regulations on banking transactions. The resultant output is due early July. A favourable outcome will improve the conversation that can be had with the banks.

The delivery of these solutions will enable POL to achieve the Reports of Compliance required as Merchant and Banking Services provider.

2. The Data Audit of our systems estate has now complete. There no additional finding reported; the full report is due to be issued by the end of the month. The remedial activities will be incorporated into the target operating model activities.

3 The PCI Programme Target Operating Model is looking at all routes for non-compliance and improving the vetting of those activities. These will include but are not limited to, training, change process changes to incorporate PCI compliance checkpoints and card data scans. One hundred and three products and seventeen processes are being analysed to establish their PCI compliance status, the analysis will be available in a month; however, with the adoption of agile method progressing remediation will run in parallel with ongoing investigation.

3. The overall timeline to regain PCI Compliance – that is, receiving Reports of Compliance for both Merchant and Banking services - is forecast between Q2-Q4 2020. While the deployment of pin pad refresh element of P2Pe is understood, and

POL00423568

underway, Post Office is reliant on Ingenico providing a plan – this is an entirely new development for Ingenico, and we are working with their senior executive team to influence their prioritisation and allocation of critical resources to the development of this solution.

POL00423568

Cyber Security Update

Author: Tony Jowett Sponsor: Rob Houghton Meeting date: 4th July 2019

4

Executive Summary

Context

In this paper we outline the progress we have made across the Cyber Security team covering changes to the team, progress on identification of critical assets, progress on the Security Transformation Programme and highlights of the recent Business Continuity Management test in Finsbury Dials.

Questions this paper addresses

- How has the scope and organisation of the Cyber Security team changed?
- Where are we in understanding the POL critical assets and data (crown jewels) and what are we doing to plug any gaps in our knowledge
- What progress have we made on implementing the Security strategy through the IT Security Transformation Programme?
- What are we doing to reduce Business Continuity Management (BCM) related risks?

Conclusion

1. The new CISO function will cover all facets of Cyber Security including Information Security, IT Security and Business Continuity Management (BCM). This will enable a more end to end governance approach to Cyber security across the domains highlighted by the recent Deloitte Report and aligns with industry best practice.
2. We have an agreed list of crown jewel data assets across all 3rd parties. We are aligning our list of crown jewels with a list of critical business assets held by the business continuity team to achieve a single view of the truth. We are hiring a data analyst and procuring a data analysis tool to further assess and discover data assets.
3. The IT Security Transformation Programme (ITSTP) has developed further to encompass all Cyber-related change covering the Deloitte Audit recommendations, including further maturity and implementation of Data loss prevention (DLP) tools , improving our 3rd (and 4th) party security assurance, and increasing the maturity and reach of the Security Operations Centre (SOC). An initial drawdown of funds has been requested with a further funding submission scheduled for end of Q2 2019/20. The investment articulated above will ensure that the most pressing Cyber risks will be mitigated in the next 12 months, aligning with Deloitte report recommendations.
4. The Cyber team has been working closely with colleagues across the business to understand and mitigate the risks associated with Information Security and Business Continuity Management (BCM).

Input Sought

The RCC is requested to note the progress made and provide feedback on the report.

POL00423568

Report

How has the scope and organisation of the Cyber Security team changed?

1. In line with the Deloitte Review and industry best practice the scope of the Cyber Security Team has been expanded to cover not only IT Security but also Business Continuity Management and Information Protection. The scope of the organisation will continue to adapt over the coming months in line with the requirement to manage the Cyber risks associated with the whole of POL organisation, 3rd parties (and indeed their 3rd parties).
2. As a result the team now consists of Tony Jowett as CISO, David Meldrum as Head of IT Security, Jules Harris as Head of Information Protection and Tim Armit as Head of Business Continuity Management.
3. The team are working with the project teams and the Third-Party Supplier teams to ensure the delivery of all aspects of the Security Strategy through the IT Security Transformation Programme.
4. Tony is prioritising meetings with the key 3rd parties to understand and align on security provision. A review of cyber governance across the organisation and 3rd parties has been instigated to ensure rapid identification and resolution of issues.

Where are we in understanding the POL critical assets and data (crown jewels) and what are we doing to plug any gaps in our knowledge

5. Post Office has been undertaking several initiatives over the last year, in order to determine what its critical data and systems are, where critical data is located, and what controls are in place around these. This piece of work has been named the Crown Jewels initiative. The initiative took as its input the definition of Data Owners by the Data Centre of Excellence (DCoE), details of systems which hold personal data from the GDPR programme, details of the criticality of systems as defined by the Business Continuity Business Impact Analysis (BIA) exercise run in 2017 and increased scrutiny of the security applied by our suppliers (who hold and process our Crown Jewels and data) through a significantly improved Information Security Supplier Management Framework.
6. A comprehensive list of Crown Jewel systems has been identified based on the information already available within IT. These are all managed by suppliers who are already part of the Information Security Supplier Management Framework. The controls in-place are deemed suitable for the data that is held after a review of the evidence surrounding these controls.
7. The next step is to check these outputs against the business view of criticality contained within the Business Impact Assessments from the Business Continuity Management team. These contain a view of criticality from a different perspective than that already covered by the analysis to date.
8. The consolidation of data from all sources will inevitably change this list of suppliers who hold Crown Jewels. Any additional suppliers will be brought into the Supplier Management Framework over the coming months.
9. On data, we mentioned in the previous report that we were investigating unstructured data across the POL administration estate. We have done an initial scan of a sample of the data and found no issues. However, recognising the importance of this area and needing to complete the analysis, we have taken the following further actions:

POL00423568

a. We have employed a data analyst who started work on 10th June with the aim of discovering the unknown unknowns connected with our data
b. We are shortly to make the decision on the selection of a tool for scanning, classifying and ultimately blocking unstructured data as appropriate as part of our Data Loss Prevention (DLP) project mentioned in the IT Security Transformation Programme update below.

What progress have we made on implementing the Security strategy through the IT Security Transformation Programme (ITSTP)?

10. Since the previous report the scope of the ITSTP has confirmed as:

    a. All recommendations from the recent Deloitte Audit Reports both Maturity and IPA
    b. DLP
    c. Increasing the reach and Maturity of the SOC including exploiting RSA Archer for increased Governance, risk and controls
    d. Increased 3rd party assessments

    A Programme plan with milestones and reports is in place with all projects on the plan with exception of those that have yet to start (e.g. DLP and further exploitation of Archer)

11. Work is progressing on all recommendations of the Deloitte Audit Reports activity. With regards to the Deloitte Maturity Assessment, seven out of the ten key recommendations have now been agreed to be completed by POL Internal Audit.

12. The remaining key Deloitte Maturity Assessment activities are

    a. To confirm cyber risks and appetite – in progress with a targeted board sign off in September 2019
    b. To agree and implement a Cyber Threat Intelligence (CTI) framework – in flight and expected to complete Q3 2019
    c. To fully document BCM process and procedures – in flight expected to complete Q2 2019

13. The ITSTP team are tracking progress on all of the detailed recommendations from the Deloitte Maturity Assessment. In addition to achievement of tasks the team are also tracking the perceived impact on maturity over time. The team have developed their own assessment method based on the values presented in the report and the number of tasks required to go from current to target maturity so that we are able to link the programme to expected maturity level increases.

14. Based on this assessment the gap between the current and target maturity levels of POL has been reduced by 23% since the start of the programme in March 2019. Key areas where improvements have been made include incident and crisis management, patch and vulnerability management and processes around secure software development.

15. For the Deloitte Information Protection and Assurance Audit then the gap between current and target maturity levels of POL has been reduced by 25% since the start of the programme. Key areas contributing to this improvement are in identity lifecycle management and user access control

16. On DLP, platform selection and initial commercials are in progress having performed pilot tests with two short-listed technologies.

17. On SOC maturity RSA Archer initial commercials are in progress. We have continued to improve the coverage and capability of the SOC. Work is ongoing with Payzone, Post Office Insurance, Accenture CDP, Branch Hub and Fujitsu to plan and design the integration of their security logs with the Post Office SOC. These areas will increase the visibility for the Post Office Security team across the Post

POL00423568

Office estate. Security alerts will be managed and co-ordinated through the Post Office SOC invoking the CSIRT (Cyber Security Incident Response Team) process where required.

18. We have commenced regular Security reviews with our major suppliers to assure they are governing themselves in line with our Cyber Security policy and Standards. In addition we will be implementing the RSA Archer Third-Party Risk modules in June to improve the overall visibility of our Third-Party vendor risks. The questionnaires that were completed initially in OneTrust by the suppliers and the manual reporting that has been used to date will be ported into RSA Archer to ensure one source of the truth for the Third-Party security risks.

19. We have also recently implemented Recorded Futures as our Threat Intelligence partner which provides additional Third-Party Risk scores that can be used within RSA Archer.

What are we doing to reduce the BCM-related risks?

20. We implemented a Business Continuity Management test using "Text blast" communication to all Finsbury Dials staff.

21. In most major cities security services have advised that large groups or personnel gathering post building evacuation presents a more obvious and accessible target than the building itself does. As such implementing a "starburst" approach to evacuation is the new recommended approach. This enables staff to disperse safely in all directions on evacuation and does not present a simple secondary target. It essentially reduces risk to life of those evacuating the building.

22. Before the test we arranged for staff mobile phone details, with their consent, to be loaded to Grapevine, our external security company, who set up text blast lists. All staff were briefed to ensure they must move at least 100m away after an alert and await the text instructions. This approach is in place for Finsbury Dials, Chesterfield, Supply Chain and the branches and will be rolled out to other locations.

23. The benefits of such an approach are that it reduces the secondary risk, ensuring that we can contact all staff who are included on the lists, and also to ensure staff can report back they are safe. For example In the recent fire test at FD over 400 staff reported back they were safe very soon after the evacuation. In a real incident this would mean we only had to follow up on the smaller number who had not replied. Floor clearing by marshals is a good tool but cannot be fully relied upon, for example when the building itself is unsafe for whatever reason. Also, it does not positively report on staff safety, rather it reports on the building being empty.

24. Overall the results showed that this is a simple, easy to manage approach which is proven around the world to support staff in a crisis.

25. Next steps to continually improve this approach include:

    a. There is further need to ensure staff instinctively understand how to respond to an evacuation and to trust that the texts will arrive as there was some chatter from staff regarding what they needed to do why they hadn't received a text etc.
    b. Some detailed technical lessons were learnt in this exercise which are being resolved
    c. The need to be able to simply know who has come into our buildings requires further work
    d. The need to implement an "invacuation" solution (building lockdown and securing when there is a major incident outside) is being worked on.

POL00423568

Cyber Risk Appetite Report

Author: Jenny Ellwood/David Mann Sponsor: Alistair Cameron Meeting date: 4 July 2019

4

Executive Summary

Context

This paper provides an update on the review of the risk appetite for Cyber/Data Security Risk and to seek approval of the refreshed and enhanced statements, methodology and plans to further pilot this approach.

Questions this paper addresses

- What is the need/opportunity?
- What has been the approach?
- What is the revised proposal?
- What are the next steps?

Conclusion

- A review of the existing Data Risk Appetite Statement has been carried out and a recommendation is made to introduce a new Cyber Risk/Data Security statement.
- A new approach has been developed which helps operationalise the Board's appetite statements. It sets a simple method for managers to assess the risks they face against agreed Likelihood and Impact scores.
- Existing MI/KPI and KRIs have been identified and a dashboard has been created to monitor performance against appetite.
- We believe this approach provides a simpler way to identify, manage and report to the Board on our risk exposure.
- Once approved we will move to pilot further risk appetite statements. We propose 'Technology' and 'People'.

Input Sought

Approval is sought to the revised risk statement, the supporting methodology and continuation to pilot this approach with two further risk appetite statements.

POL00423568

4

The Report

What is the need/opportunity?

The Need

1. The Risk Appetite Statements (RAS) approved in 2015 have been reviewed. Whilst broadly accurate, the statements are very high level, difficult for the business to interpret in their decision making process and to monitor whether they remain 'within' or 'outside' of risk appetite.

2. The Risk and Compliance and the Audit & Risk Committees have asked that the RAS are reviewed and refreshed. Whilst a recent Cyber Security Internal Audit review also recommended a revalidation of the Cyber RAS to ensure it mirrors Board expectations and can be translated into operational activities.

The Opportunity

3. A review of the RAS not only provides an opportunity to validate and recommunicate the Board's appetite expectations but also helps drive risk-based discussions and decision making across the business.

4. Through the use of agreed MI/KPI/KRIs, risk appetite can be quantified and allow senior management to assess risk and determine if they are 'within' or 'outside of risk appetite' and take appropriate action.

5. When fully reviewed, refreshed and embedded RAS will help provide a more 'metric' driven view of how we are performing against risk appetite enabling the Post Office and its Board to focus attention on areas deviating from the agreed appetite and direct/intervene if required.

What has been the Approach?

6. A review of the Cyber Risk/Data Security RAS has been undertaken with IT to align the current threat landscape. Multiple workshops and challenge sessions resulted in:
   - A proposed new Cyber Risk/Data Security RAS
   - A new Risk approach which 'operationalises' the Board's appetite statements
   - A simpler method for managers to assess the risks they face against an agreed Likelihood and Impact score
   - Faster and more accurate identification of where a risk may be 'outside' appetite' and requires further mitigation
   - Identification of when a risk requires escalation
   - Simpler reporting within functional risk management meeting (i.e. ITLB)

7. The steps taken were as follows:

POL00423568

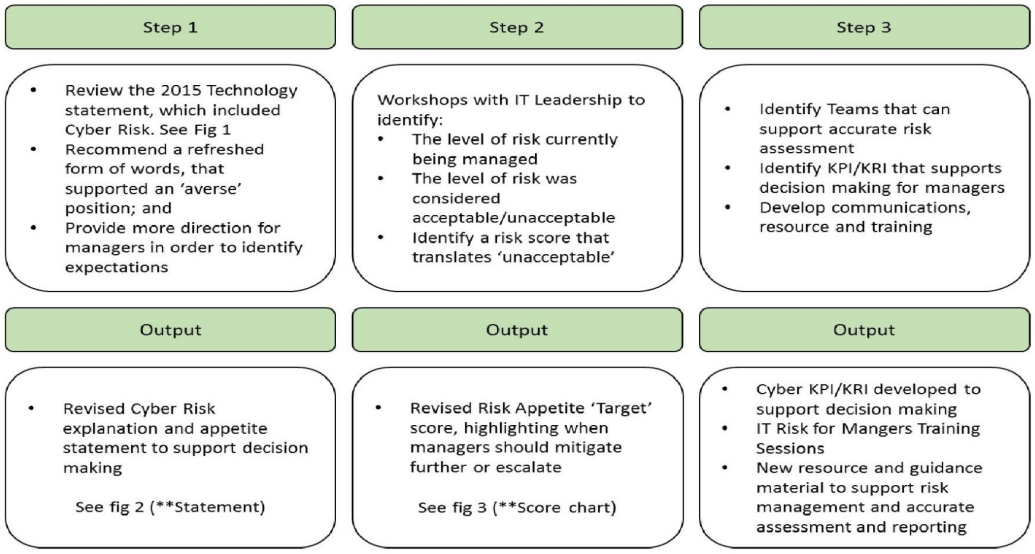


Figure 1: 2015 Relevant Risk Appetite Statements

Principle Risk	Appetite
Technology Systems and IT related risk; stability, design, implementation. This also includes IT Security, hacking, and unauthorised use of data.	Averse risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences

NB: The 2015 statement was positioned to include areas such as, stability, design and outages and was not Cyber/Data Security specific.

Figure 2: Revised Cyber/Data Security Appetite Statement



Figure 3: New Target Score for Cyber/Data Security and additional guidance for Managers

Impact Score	Label	Financial** (EDITDAS)	Operational Continuity (Operations, IT, Colleagues)	Reputational (Stakeholder, Customer, Colleagues, Third Party, Media, Regulator)	Likelihood Score	Label	Probability	Final Score
2	Moderate	>1-5% of financial target or significant impact on all objectives	Local service disruption at several locations or business functions for >3 days	Moderate concern from stakeholder/ customers/ colleagues/ 3rd party support, or - some local media coverage, or - informal regulatory conversations	2	Unlikely	>10-25%	4

Due to the **motivations and skillset** of those who would attempt to do us harm, it is **possible that incidents could impact our business**. Also, due to the **complexity of our IT systems and vendor/contractual relationships**, it is **not always possible to guarantee that we are at the cutting-edge of security practices**.

IT will continue to invest in ensuring activities do not place our data in harms way and work to **prevent/mitigate the impact** of any attack through **effective security defences**. In managing these complexities, IT continue to create an environment where it is **unlikely** that any decision or activity will present more than a **moderate impact**.

POL00423568

4

What is the revised Proposal?

8. We propose that the 2015 RAS (see Figure 1) is replaced with a more specific Cyber/Data Security RAS (see Figure 2).

9. We have considered the harm table and what the regulator would consider to be the correct 'target' impact/probability score. This enables the business to understand what the term 'averse' translates into (see Figure 3).

10. This has been expanded to include a statement of intent. This confirms that whilst it is possible that an incident could impact our business, IT will continue to invest in ensuring activities do not place our data in 'harm's way'. It then confirms that IT will continue to create an environment where it is unlikely that any decision or activity will present more than a moderate impact. This should help prioritise business change decisions.

11. Whilst a preferred Cyber Risk score would be very low, we do not believe a 1 by 1 is reasonable due to the nature of cyber risk and the ever changing threat landscape. That said, a regulator, such as the ICO, may not accept an 'Amber' target. Given these competing perspectives the CISO/DPO's collective view is that whilst a 'Green' position may be hard to achieve, it presents a clear statement of intent to protect data and ensures that risk remains high-profile within the organisation.

12. Therefore, the recommendation is that we maintain a 'Green' target and an 'averse' appetite for compromise or loss of data. In real terms the Cyber/Data Security journey looks like this:

Inherent Risk	Residual Risk	Target
It is generally accepted that organisations face a 'High' risk from Cyber criminality or the impact of Data Loss.	Our position with the controls we are currently applying across POL and linked with IT's Security Transformation Programme.	Our appetite for data loss/compromise and the position we are aiming to achieve to protect our customers, colleagues and business.

13. A scorecard has been developed to track how Post Office is performing against Risk Appetite for Cyber and Data Security (see Appendix 2)

What are the next steps?

14. If approved the next steps with Cyber/Data Security RAS is to communicate it across IT and Information Security to ensure colleagues who either manage Cyber / Data Security or who make business decision around it are aware of the revised statement and what it means to them.

15. The Post Office's Information Security Committee (ISC) will use the new RAS and supporting process to assess new/existing risks and recommend remediating actions as appropriate.

16. In terms of the wider business, the Cyber and Information Security policy, existing communications and training material already make clear we have

POL00423568

a low risk appetite for data loss and we will continue to communicate this message across the business and with 3rd Parties.

17. The policy confirms: *'Post Office's Board and Group Executive (GE) recognise that cyber and information security threats present significant financial and operational risk to Post Office its, subsidiaries and associated entities. The GE are committed to developing a strategic response to current and emerging threats to enable Post Office to achieve its objectives, whilst preserving Post Office's brand, commercial image, reputation, competitive advantage, revenues, profitability, legal, regulatory and contractual compliance'*.

18. The Central Risk team will follow the steps/methodology shown in paragraph 7 to review the Technology and People RAS and again bring the results and recommendations to RCC and ARC for validation and approval. If this approach works for those appetite statements a plan will be developed to review all remaining appetite statements so that a full set of approved revised statements with supporting metrics are in place for the Post Office.

POL00423568

Appendix 1: Risk Appetite Descriptions

Risk Appetite Approach	Risk seeking	Risk tolerant	Risk neutral/balanced	Risk averse
Risk taking vs. reward	Post Office actively encourages risk taking	Post Office is willing to take greater than normal risks	Post Office takes a balanced approach to risk taking	Post Office actively discourages risk taking
Objective/negative impact relationship	Willing to accept a significant negative impact in order to pursue objective	Willing to accept some negative impact in order to pursue objective	Potential negative impact and objective given equal considerations	Not willing to accept any negative impact
Impact on residual risk	Post Office will accept high levels of residual risk in pursuit of its objectives	Post Office will accept some residual risk	Residual risk will be balanced against potential business benefits	Post Office will mitigate/treat risks in order to minimise residual risk

POL00423568

Appendix 1: IT Security KRI Scorecard

Risk Statement	Target Criteria	BiMonthly Target	Jan/Feb 19	Mar/Apr 19	May/Jun 19	Cumulative Status
Lack of POL Security Improvement Plan	Sign off by ARC	Approval	Approved	Approved	Approved	Effective
Inadequate security review/signoff	All Change Requests reviewed	100%	100%	100%	100%	Effective
Outages generated through inadequate security controls	Number of outages	0	0	0	0	Effective
Lack of Compliance to Security Policies & Standards	Compliance dip sample via ISMF's (no of vendors)	2	N/A	N/A	N/A	Not Started
Compliance with Third Party Vendor Management Framework	ISMF's completed as per schedule (% completed)	100%	100%	100%	100%	Effective
Lack of JML Process	Quarterly AD Reconciliation with Success Factors	Completed	N/A	N/A	N/A	Not Started
Lack of JML Process	Quarterly reviews of critical systems	Completed	N/A	N/A	N/A	Not Started
Inadequate Identification & Remediation of IT Vulnerabilities	Vulnerabilities remediated within Policy	Yes	No	No	No	Challenged
ITCF Management	Quarterly compliance check completed (Apr/Jul/Oct/Jan)	Completed	-	Yes	-	Effective
Compliance to GDPR Training	Internal GDPR training completion (% of nominated staff)	>95%	Yes	Yes	98%	Effective
Compliance to Information Security & Data Protection Training	Internal compliance training completion (%)	>95%	Yes	Yes	98%	Effective
Compliance to ISO27001 Certification - Surveillance Visit Passed	Bi-Annual Surveillance Visit (2 per annum)	Pass	Pass	-	1 Minor	Effective
Compliance to PCI-DSS V3.2 Certification - Internal	Internal quarterly review completed	Yes	Yes	-	-	Effective
Compliance to PCI-DSS V3.2 Certification - Annual Certification Passed	Annual certification passed	Pass	N/A	N/A	N/A	Report Not Due
Remediation of Deloitte security audit findings	% of findings completed by due date in quarter	100%	N/A	N/A	N/A	Not Started
Identification of Internal Accidental/Malicious Actors	Ironscales Phishing Reporting (% failures)	0%	0%	0%	0%	Effective
Inadequate Threat Intelligence, Scanning & Analytics	Monthly Review of Threat Intelligence/ASOC Alerts	2	2	2	1	Effective
Lack of ASOC Capability	Monthly Review of ASOC Reporting	2	2	1	1	Effective
Identification of External Malicious Actors	Bi-Monthly review and ASOC fine tune completed	2	2	2	1	Report Not Due
Inadequate CSIRT Capability	Playbook design completed	1	0	1	N/A	Effective
Inadequate CSIRT Capability	Desktop exercises completed (2 per annum)	-	0	0	1	Effective
ITDR testing of Critical Post Office systems	Number of ITDR tests completed against target	100%	62.50%	37.50%	83.30%	Challenged

POL00423568

POST OFFICE LIMITED
RISK & COMPLIANCE COMMITTEE

Cash Management System Upgrade - review

Author: Benjamin Cooke, Russell Hancock **Sponsor:** Rob Houghton **Meeting date:** 4th July 2019

Executive Summary

Context

5

IRRELEVANT are a software company who licence and support the application Post Office uses for cash logistics and processing operations. It is a critical application for Post Office. If the system was unavailable for 2 hours in the morning, cash deliveries and collections from/to Post Office branches would have to run through manual contingency processes. We would struggle to forecast expected branch cash requirements and cash holdings would be calculated based on last recorded amounts, plus manual adjustments.

The IRRELEVANT application implementation contributed to Back Office Transformation project delays. The decision to Go-Live was taken knowing that not every cash transaction recorded in depots was flowing through to the finance system. Their delivery capability is limited and continues to constrain project delivery. We are reviewing IRRELEVANT architecture and delivery capability. This paper outlines the residual risks with IRRELEVANT and the steps management are taking to mitigate operational, financial or branch risk.

Questions addressed in this report

1. Who are IRRELEVANT and what do they do for Post Office?
2. Could Post Office have applied more rigour to key decisions? What lessons can we learn?
3. What are the current risks to Post Office and what are our mitigations?
4. Why do we believe it's worthwhile continuing to invest in Transtrack?

Conclusion

- IRRELEVANT is a critical application for Post Office supporting our Supply Chain cash and logistics capability.
- The decision in 15/16 to use IRRELEVANT rather than POLSAP could have had more scrutiny. This was potentially due to the urgency of migrating away from POLSAP and lack of technical skills and capacity within Post Office. The decision may still have been taken to select IRRELEVANT however more technical due diligence may have mitigated operational and development risks.
- The financial reconciliation issue is still not resolved, albeit improved significantly since Go-Live. Our teams are ensuring that our financials are robust and that there is no impact on branches. Concurrently controls are being put in place to

POL00423568

prevent similar issues, but also spot and remediate in the case future technical issues did arrive.

- The Supply Chain teams' efficiency using IRRELEVANT is improving as they become more familiar with the application. Provided we continue to see progress in mitigating the downsides, we see IRRELEVANT remaining a critical application partner.

The Report

Who are IRRELEVANT and what do they do for Post Office?

1. IRRELEVANT are a small software company focused entirely on currency logistics and management technology, recently acquired by IRRELEVANT a larger Germany firm who primarily sell currency machinery, and provide Post Office's Bank of England approved high speed note counters. Post Office first procured IRRELEVANT Cash-in-Transit (CiT) system in 2005 and it has been used by Supply Chain ever since to track pouches of cash (and other valuables) on our secure van routes from depots to branches and back.
2. In November 2016 the board approved Back Office Transformation, which proposed to design out POLSAP, rather than upgrading. POLSAP was used to manage cash logistics in Supply Chain counting centres. Rather than migrate to another heavily customised SAP solution, the decision was taken to adopt functionality from IRRELEVANT module designed for this purpose. From February 2019 Post Office's entire Supply Chain cash processing and logistics has operated entirely using IRRELEVANT applications. A timeline of key events is provided in the appendix.

Could Post Office have applied more rigour to key decisions? What lessons can we learn?

3. This paper focuses on the two more recent decision points, firstly the decision to select IRRELEVANT as the application for cash processing, and secondly the decision to develop further forecasting capability, rather than go to market for a best of breed forecasting solution.

Cash Processing Application

4. POLSAP was a critical part of Post Office. Without it clients could not be paid and the cash supply chain would have ceased to function. Failures had already occurred, SAP extended support was ending and Fujitsu were unable provide any SLAs around infrastructure. The cost of upgrade was estimated at £6m and would have left Post Office continuing with unsatisfactory processes. In November 2016 the board approved an approach that proposed to design POLSAP out, migrating processes to other systems. A key early deliverable was a Supply Chain strategy and application options review, the options being considered were using a SAP technical service to migrate POLSAP custom code into our SAP CFS financial

POL00423568

system, migrating to IRRELEVANT or starting a 3rd party application procurement.

5. *Technical SAP Migration* - Post Office and Accenture worked with SAP's technical team to assess options to segregate POLSAP's cash supply chain processes from the financial and migrate the custom supply chain code into CFS. A study document was provided laying out technical options and effort costs for the SAP technical work. The project team then assessed the additional work required from Accenture and Post Office and risks with the approach.
6. IRRELEVANT invested a couple of months to create a "quick scan report" reviewing how closely Supply Chain processes fit to the IRRELEVANT application. The project created a "IRRELEVANT High Level System Assessment" and visited two IRRELEVANT client sites to see the system in operation.
7. *3rd Party Procurement* – The timeline required for a 3rd party procurement prior to starting migration was deemed too long to seriously consider with the state of POLSAP.
8. The team report a decision was made to select IRRELEVANT in a Steering Committee or Project Delivery Group meeting, however whist a decision document was drafted and requirement gathering began with IRRELEVANT it isn't recorded formally in any meeting.
9. There were a number of lessons learned on technical due diligence, partner management and governance.
10. *Technical Due Diligence* - Post Office's largest cash counting sites are 5x larger than IRRELEVANT next largest customer. Whilst the Cash in Transit (CiT) application had been performing at Post Office scale for some time the application architecture of IRRELEVANT is entirely different. A new vendor would have been asked to confirm performance metrics and been subject to a more thorough set of technical questions. The IT architecture team has increased significantly since 2016 and is now engaged in all major technical change decisions and we have improved architecture governance reviewing all technology aspects during the procurement process.
11. *Working with smaller partners* – IRRELEVANT team within the project were treated similarly to those from large consulting organisations. However, based on the size of the organisation more oversight was required. With larger organisations/vendors A) the product and delivery capability has been tested more thoroughly and B) in the case of issues talent can be re-prioritised by management to assist. When IRRELEVANT started to struggle it took the project team too long to realise, there was not the strength and depth within the project team to cover gaps, and it belatedly fell on Post Office to assist in helping improve IRRELEVANT internal capability. Under the revised Change Excellence Framework we have re-introduced periodic independent health-check assurance reviews for the largest programmes, these are being undertaken by the Change Risk & Assurance Team. The Strategic Portfolio Office are also reviewing progress of major programmes monthly and commissioning health-check assurance reviews as required. This central oversight should help identify problems earlier.

POL00423568

12. *Formal decision documentation* – Although a decision was made within the Back Office Transformation programme it had a significant impact on IT, Finance and Supply chain and should have been better documented and likely noted to the GE.

Cash Forecasting Application

13. Having evaluated the basic forecasting capability within IRRELEVANT it was clear that additional features were required, yet Post Office's requirements were relatively basic compared to most retailers. Two options were considered: procuring a best of breed forecasting solution, or co-developing additional features within IRRELEVANT
14. Post Office worked with a specialist supply chain consulting firm to evaluate options and get to a recommendation that the Supply Chain team supported.
15. The decision was recommended by the Cash Processing Project Delivery Group (PDG) then approved at Steering Committee.
16. In this case the decision making process was robust, and due consideration was given to working with a smaller firm. Issues and lessons learned relating to the design, build and attempted deployment are covered in the programme lessons learned.
17. It should be noted that PO instructed IRRELEVANT to pause its development in order to focus on getting the core elements live, with a combination of manual forecasting and an interim solution using Power BI being developed in-house.
18. Since go-live forecasting has been performed manually, with Power BI interim solutions going live in May.
19. The inventory management team have brought stock holdings down to levels prior to IRRELEVANT migration successfully using manual forecasting. This is however labour intensive
20. An options paper is currently being written looking at options for the future of forecasting. Transtrack being one of the options.

5

What are the current risks to Post Office and what are our mitigations?

21. The key risks being monitored relating to IRRELEVANT are outlined in the table below.

Risk Title		Likelihood	Impact
Description	**Mitigating Action**		
There is a risk of **inaccurate financial reporting** due to cash movements in depots recorded in IRRELEVANT not always being sent to our financial system.		**5**	**4**

POL00423568

Risk Title		Likelihood	Impact
Description	**Mitigating Action**		
Since February 2019 the IRRELEVANT system has not been sending all financial transactions to CFS. At year end CFS was understated by IRRELEVANT at peak this increased to over IRRELEVANT and around IRRELEVANT transactions. The project team and IRRELEVANT reduced the daily failure rate to ~ 20 missing transactions a day from May, and have re-processed the bulk of missing historical transactions. Currently CFS is overstated by approximately IRRELEVANT, with the figure continuing to reduce as the project clean-up continues. Even with 20 missing transactions a day, a fairly significant manual overhead is required from the Post Office business to ensure no impact to Post masters or financials.	• Technical progress is being made on solving this issue after Go-Live around IRRELEVANT of transactions were missing every day, this figure is now IRRELEVANT (around 20 transactions). • Supply Chain conduct physical cash counts weekly to ensure actual cash matches IRRELEVANT depot cash-on-hand • The BOT project team remain in place running regular reconciliations and tracking all missing transactions. This activity is being handed over to BAU. • The re-processing of historical missing transactions has cleaed the bulk of the IRRELEVANT with around [redacted] remaining. These remain stuck due to a number of underlying root causes. These are now each being investigated with plans created to tackle each. •		
There is a risk of future **inaccurate financial reporting**, due to IRRELEVANT application architecture allowing the types of errors causing the issue above.		**3**	**4**
There is a risk that once the initial issues have been fixed, IRRELEVANT IRRELEVANT in future fails to send all transactions to SAP CFS leading to our financials again being out of sync.	• An on-going process for financial reconciliation is being put in place to ensure this issue would be spotted. • Financial reconciliation is being handed over to BAU along with tools to automate as much as possible, quickly pin-pointing any missing transactions. •		
There is a risk that Post Office **Supply Chain operations are interrupted** in future due to IRRELEVANT application failures, and IRRELEVANT are unable to quickly diagnose and fix due to issues with IRRELEVANT application architecture and delivery capability		**2**	**4**
Challenges through back office transformation have exposed flaws in the IRRELEVANT application architecture, their development capacity, deployment approach and skills. There is a risk of future service disruption, possible performance degradation as Banking Framework increases and that Transtrack will struggle to resolve issues in a timely fashion.	• Small issues already exist and are being resolved slowly, interrupting supply chain. Any larger issues faced (outside of the financial reconciliation issues) have received high focus from IRRELEVANT and been resolved quickly by the support team. • Accenture technical specialists have been engaged to conduct an architectural review. IRRELEVANT are actively supporting the exercise. • Following report delivery a set of improvement actions are being agreed with Transtrack that will continue to be reported against over time in monthly service reviews		

POL00423568

Risk Title		Likelihood	Impact
Description	**Mitigating Action**		
It is also worth noting that IRRELEVANT have just been acquired by IRRELEVANT which may impact their ability to delivery. This is an opportunity as much as a threat and is being closely watched with the Post Office Supply Chain Director and Back Office IT Director engaging closely with the IRRELEVANT and IRRELEVANT leadership through the process.		2	3

5

Why do we believe it's worthwhile continuing to invest in IRRELEVANT

22. Whilst project delays have been frustrating Supply Chain did entirely cut-over to IRRELEVANT at the end of January 2019. All cash depots, coin stores, inventory management and CViT drivers have been successfully operating on this single integrated platform since that point with no major operational issues. The teams are fully trained with the scrutiny brought by the financial reconciliation challenge helping to force all units to have a deep understanding of how the application works.
23. Technical performance has recently been re-checked under live environment and other than a couple of known issues soon to be fixed, the system meets our expectations.
24. Inbound processing at our Supply Chain depot in Belfast – the first to Go-Live on IRRELEVANT – has stabilised at around 14 pouches per hour. Higher than the 11 pouches per hour recorded when they used POLSAP, a 27% productivity improvement. As other sites become used to the system we are seeing performance steadily improve and they are now approximately equal to their POLSAP pouches per hour.
25. IRRELEVANT recognise that where their application has not met the quality standards they set, their effort to resolve performance issues or bugs is covered under application warrantee and hence they are not charging Post Office. Their team is motivated to work for Post Office – their largest customer – and they do so proactively and with passion.

POL00423568

Appendix

Timeline of Events: IRRELEVANT

Year	Event	Description
2005	Post Office IRRELEVANT CViT bought	Post Office tenders for a CViT application for Supply Chain and IRRELEVANT wins
2015	Post Office IT moves to a SIAM tower model	IRRELEVANT is defined as a back office application. Accenture wins Back Office tower hence IRRELEVANT is planned to novate IRRELEVANT into the Accenture Back Office Tower.
2016	IRRELEVANT CViT Upgrade	In June a project goes live upgrading IRRELEVANT CViT moving away from a distributed hardware at depot model, to a central instance. This stops all the site failures due to old hardware plaguing supply chain. The upgraded, stable system is well received.
2016	IRRELEVANT is paused from on-boarding to the Accenture back office tower	In August a decision was taken not to migrate IRRELEVANT and novate to Accenture as: 1. the project had barely started engagement, 2. the system had only just stabilized for Supply Chain 3. Accenture raised a number of concerns about novating the contract as it didn't meet the standards Post Office required from Accenture and the contracted scope was wrong, leading to significant additional cost.
2017	Decision taken to migrate POLSAP Cash Processing functionality to IRRELEVANT IRRELEVANT	In early 2017 the Back Office Transformation program team and Supply Chain recommended migrating from POLSAP onto IRRELEVANT module, purpose built for Cash Processing.
2017	Decision taken to custom build additional forecasting functionality in IRRELEVANT (rather than 3rd party best of breed)	Crimson assisted with a piece of work reviewing the proposed forecasting solution. They indicated that there was a gap – that could be filled by a best of breed, or some custom development. A follow-on piece of work evaluated these options and in the end (mid-November) recommended proceeding with IRRELEVANT
2018	Forecasting implementation put on-hold	As the forecasting functionality could not be demonstrated to work using Post Office data, any effort to deploy has been put on hold since Sept 2018

5

Strictly Confidential

POL00423568

Risk, Compliance and Audit Report

Author: J Ellwood, J Hill, J Appel Sponsor: Al Cameron/Ben Foat Meeting date: 04 July 2019

Executive Summary

Context

This paper provides an update on the key and emerging risks and issues that Post Office is managing and an update on the latest Audit position.

Questions this paper addresses

- What are the key risks and compliance issues and what is the business being done to address these?
- What are the emerging risks we face in both the short and medium term and what are we doing to address these?
- What is the status of the Change Portfolio and its current top portfolio risks and key delivery challenges?
- What is the forward-looking regulatory agenda and key policy updates?
- What progress has been made with the internal audit plan and what key messages have been reported?

Conclusion

- The paper provides an update on the following top risks PCI, Information Security, GLO, People, Brexit and Payzone Payment Device vulnerabilities.
- There have been exceptions approved this month for Branch Hub and Parcelshop. The number and type of significant incidents continue to follow a similar trend as previous months.
- System requirements for Archer (GRC tool) have been scoped and shared with 2MC (implementation provider). A prototype will be built and used to test, along with a roadmap and implementation plan.
- The Compliance heat map is provided in Appendix 5. Key points to note are that Data Protection has reverted to Amber from green due to remedial work identified from the GDPR Gap Analysis. A separate paper is provided on this.
- Additionally, the status of Financial Services Compliance and Conduct has also moved to Amber due to the instances of non-conformance identified through mystery shopping.
- Eight internal audits were finalised since the May RCC, none of which have adverse report ratings. Reports summaries are provided from paragraph 66.
- The 2018/2019 internal audit programme has now been delivered in full. Observations from all reviews have been analysed and recurring control themes are reported from paragraph 59.

Input Sought

There are no decisions required at this time. The Committee is requested to note this paper.

POL00423568

The Report

Risk

Author: Jenny Ellwood

What are the key risks facing the business and what is being done to address these?

1. The heatmap has been updated to reflect recent business structure changes within Legal, Compliance and Governance, CISO (incorporating Info Security risks) and CFO to include Risk and Audit risks (see Appendix 1). Legal and Regulatory and Strategic are the principal risk categories which continue to report red and where there is continued focus on actions.

2. Since May, risk descriptions and mitigations have been reviewed and marginal changes have been made to the Top Risk profile (see Appendix 2), scores for the period remain stable.

3. The PCI risk continues to report red (4:4) and a separate update from Rob Houghton will be provided in July's meeting. There are challenges with Ingenico regarding timeline and cost of the new solution. However, the pin-pad preparation and rollout activities are on schedule with the first refreshed pin-pads arriving in branch at the beginning of September.

4. Work continues on the IT Security Transformation Programme (ITSTP) the scope has been further developed to encompass all Cyber-related change covering the Deloitte Audit recommendations, including further maturity and implementation of Data loss prevention (DLP) tools, improving our 3rd (and 4th) party security assurance, and increasing the maturity and reach of the Security Operations Centre (SOC). 7 of 10 'high-rated' recommendations have been closed. The other 3 remain on track.

5. The second High Court trial relating to Horizon is due to conclude week commencing 1 July. Deloitte are supporting our preparations and workshops are underway to record the risks, mitigations and owners. Central Risk will review the outputs from these sessions.

6. The activities to remediate the security vulnerabilities identified within the Payzone Payment Device Penetration Test are continuing and are on-track. A Post Office review of the risk position has concluded and we believe that the overall position is Amber. This will be ratified in the Cyber Risk Workshop taking place on 1 July. Risk exposure will decrease over time as the remediation activities conclude. On the basis the plan remains on-track, all security vulnerabilities will be resolved by October.

7. A wider risk workshop to consider other risk areas i.e. strategic, operational and financial is being arranged.

What are the emerging risks we face in both the short and medium term and what are we doing to address these?

8. In terms of risk incidents for June, ATM gas attacks, branch robberies and Information Security breaches continue to trend. ATM crimes have increased

POL00423568

nationally by over 200% since last year. The Security Operations team use a risk model to identify high/medium/low risk branches for all offence types and a monthly report is tabled at Operations Board, covering the trends / spikes for these incidents. Mandatory training on Information Security and Data Protection was rolled out in June which should increase the awareness of employees, mitigating data privacy breach incidents.

9. Exceptions were approved for the Branch Hub and Parcelshop programmes. For Branch Hub an approval for a reduced user registration has been agreed which takes us outside of the IT Security Policy for a period of 3 months. A solution which aligns to our policy is in development. Parcel Shop has a small number of vulnerabilities with the hand held device used to deliver the parcel returns and collections services. The exception is for a 4 week period, interim controls have been put in place and will be reviewed regularly.

10. In terms of the commercial risk called out in May regarding Fit and Proper, the business have accepted that it may be necessary to switch off some independent branches from selling foreign currency. As work is still underway, a verbal update will be brought to the RCC meeting.

11. In response to significant people changes in critical roles and further planned organisational design changes, the review to assess the capability required of senior positions including the identification of critical roles continues. A review of career progression for staff members is also ongoing to understand current and future requirements for talent development.

12. In May, the Banking Director flagged that there has been heightened interest from the banks regarding cash withdrawal card transactions relating to a risk that transactions are not being processed correctly by the Postmaster in all cases. A system solution fix has been developed to remediate, which is currently planned to be implemented by August/September.

13. Brexit planning continues and we remain in regular dialogue with BEIS. BEIS have confirmed that 'No Deal' Plans' should be 'shrink wrapped' and businesses should plan for a 'Deal'. However, Post Office are continuing to work on some remediation activities for a 'No Deal', particularly the ongoing engagement with third parties who have not yet responded to our questionnaires. We do not believe the risk of a 'No Deal' has reduced and it is proposed the Operations Working Group is re-established to review our original contingency plans and ensure they are still appropriate. We need to also consider if there are any other major 'IT' releases or significant activities planned such as marketing campaigns during the lead up to the 31 October and the immediate time after which may create additional pressures.

14. Back in January's ARC, Risk were asked to work with Retail to consider whether we could further develop the monitoring process in place for our key multiple partners. A visit was arranged to BEIS to review their process and Karl Oliver has been working on this. Retail have developed MI, which is refreshed and reviewed on a monthly basis with the Retail Director. The multiples currently monitored are: McColls, Cooperative, WH Smiths, AF

POL00423568

Blakemore, One Stop and Tesco and additional partners can be added based on size or risk. An example of the MI metrics is included in Appendix 3.

What is the status of the Change Portfolio, its current top portfolio risks and key delivery challenges?

15. The overall status of the portfolio remains Amber. Work to address some long standing issues has resulted in a reduction of programmes which reported one or multiple Red statuses from 7 to 4. However, there still remain a number of significant projects (such as Belfast Exit and Data Analytics) where re-baselining work is required due to re-prioritisation.

16. The portfolio continues to be prioritised to ensure 3YP benefits are achieved. Financial analysis has now been made available to all project managers to enable self-serve and improved awareness.

17. Appendix 4 provides a summary of the current key 'Platinum and Gold' change programmes and their current reporting status. 4 projects are reporting Red RAG statuses. The key ones are as follows:
    - **PCI Compliance** (Costs, Delivery and Risk Red RAGs).
    - **Data Analytics Excellence** (Risk Red RAG): The programme has now been restructured with some activities under the Data Governance and Data Visualisation workstreams moving into BAU. The Business Case to build the new Data Platform and complete Credence decommissioning will be presented at PRB in July. Supplier costs and plans remain outstanding hence reporting red against risk.
    - **POCA Implementation** (Delivery and Overall Red RAGs): The WAN implementation continues behind schedule due to issues with Vodafone (a DXC subcontractor). We are waiting for an updated schedule for when the new WAN connections will go live. DXC have also confirmed the de-scoping of the mobile app. This is driven by DXC underestimating the complexity and cost of implementing the app and the short amount of time left remaining on the contract to recover their investment. The financial benefits from delivering the app are already committed in the contract so POL are not adversely impacted. The cost of delay has a small impact on POL as we will likely need to fund our project manager for additional months. This will be confirmed once an updated schedule is received. No impact expected for customer or postmasters.

18. The June Change Risk Management Group (CRMG) considered the existing 8 strategic portfolio risks. The People risk remains key (3:4) around change programmes not having appropriate resource (skills and or experience) assigned, adversely impacting effective change delivery.

19. The work to mitigate this continues with the goal of matching resources with the relevant competencies to projects which are now classified as being platinum, gold, silver and bronze. SPO is also establishing 'Practices' (for Portfolio, Programme, Project and Agile professionals) with the objective of enhancing the competency levels of both our permanent and contactor Change staff this includes implementing a best in class competency framework for assessing and developing competency level.

POL00423568

Compliance

Author: Jonathan Hill

Telecoms

Text Relay

20. Ofcom has issued a draft Section 135 notice to support its investigation into the text relay issue. On 21st June we provided the second part of the response. Ofcom has recognised the actions we have taken to fix the billing system for text relay calls, our commitment to reimbursing impacted customers and that we have self-reported, which is anticipated to help reduce any penalty the regulator may seek to impose.

21. Ofcom has indicated that it may be prepared to enter into early settlement discussions, and we have responded saying that we would be interested to explore this approach.

22. We will be compensating customers where we have data. Fujitsu is producing the data extract to enable us to identify impacted customers. Where we do not have data we will make an estimate and then make a contribution to our charity – Action for Hearing Loss.

Age Verification

23. On Thursday 20th June the Secretary of State for BEIS announced that the Age Verification has been delayed by at least 6 months due to essential documents not being put to the European Commission. This was due to have come into effect on 15th July 2019.

Data Protection

24. The GDPR programme was formally closed at the end of Q1. There is a separate paper to be discussed at RCC.

25. This year's Data Protection training has gone live for all employees, contractors and agents. The Data Protection team are monitoring progress, reminders will be sent to Line Managers to ensure that completion targets are met within the set timeframes. Further focussed training is being developed in conjunction with Learning and Development. This additional mandatory training is aimed at those employees that use or have access to bulk and/or sensitive personal data in their day to day activities such as HR, Marketing and the IT.

26. In the last quarter there have been two Privacy and Electronic Communications Regulations notifications that have been made outside of the statutory 24hr reporting period. These are likely to result in a fixed penalty notice (£1,000) being issued against Post Office Ltd. Investigations found that these were isolated incidents due to agent error within the Telecoms Call Centre. Additional training has been given to relevant personnel and awareness raised for all staff to be vigilant with reporting. Additional controls have been deployed and these controls are due to be tested in the first week of July by the Data Protection team.

POL00423568

Financial Crime

Compliance with Money Laundering Regulations

27. Between 24th April and 19th June 2019, 66 new Bureau de Change non-conformance cases were identified. During the same period 65 open cases were resolved, of which 10 related to customers who had purchased in excess of €15k in 90 days, which breached the regulatory limit and mitigating actions have been taken. There was one material breach in May where £29k was purchased at different locations by a boxing promoter.

28. Resource provided by the Data Centre of Excellence to resolve the outstanding issues with the Bureau de Change transaction monitoring system has designed and developed a number of the additional reports that had been agreed with HMRC. The Financial Crime Team are piloting these and have identified some branches where high levels of cash purchases just below £1,000 are indicating deliberate avoidance of the customer data and ID capture requirement for £1,000 and above. The reports remain operationally inefficient (this cannot be fixed in the current Credence/Business Objects solution) and will be tested over the next 6 months and implemented gradually to measure the operational resource requirements v. benefits of the new reports.

29. There is still an outstanding Credence system issue that is causing transaction record errors that is with Accenture to scope a fix.

Anti-Bribery and Corruption ("ABC") update

30. See separate report.

Whistleblowing update

31. See separate report.

Fit and Proper

32. There remains a focus on gathering full F&P returns and we continue to share data with HMRC fortnightly to evidence our progress:
    - The latest metrics suggest full compliance among our Commercial Partners will occur during July, although some chasing is still required. We currently have 29 of 43 fully complete and are actively engaged with the remainder.
    - Among the non-commercial partners, 64% are already fully compliant and another 21% have submitted responses which need work but are expected to achieve compliance during June and July. New responses are continuing to come in from the remaining 15%, albeit in small numbers. We are planning a concerted final push (via Network Area Management) on that remaining group in late June / early July.
    - It is likely that despite the efforts of Network Area Management, for some Agents it will only be formal notification of their BDC capability being revoked, or the capability actually being revoked, which stimulates engagement.

POL00423568

- With that in mind, the revoke functionality (MDM and Horizon) is being adjusted so that it can operate quickly and accurately in either direction - i.e. revoke and reinstate - which has not hitherto been the case.

33. The project is now also designing the processes/supporting systems changes required for F&P declaration to operate annually from January 2020, with agents divided into cohorts with declaration anniversaries spread throughout the year.

Regulatory updates

34. Post Office submitted a response on 10th June to the HMT consultation on the transposition of 5th Money Laundering Directive into UK law. Whether customer due diligence is required as a distributor of third party manufacturing pre-paid cards, we have raised concerns:
    - about the inclusion in the UK Politically Exposed Persons (PEPs) definition of "Board members of for-profit enterprises in which the state has an ownership of 50% of more, or where reasonably available information points to the state having control over the activities of the enterprise", which would bring Post Office Board members into scope for PEP due diligence in their personal financial dealings.
    - on the extension of the regulatory definition of 'officer' to 'managers', and that this should be 'senior managers' to align with the FCAs Senior Manager Regime
    - we are also asking the Government recognise GOV.UK Verify scheme under the provisions

External Threats

35. We continue to see a number of high value and complex cases relating to business banking deposits and are currently liaising with a number of Banking Framework Services banks to investigate. There is anecdotal evidence that some of these cash deposits are linked to the onward purchase of crypto currencies.

Internal Threats

36. Financial Crime risk assessments and re-assessments across 36 products and services have not identified any major internal threats, and the outcomes have been shared with the Risk team to ensure that any risks are identified and reflected in functional RACMs. The Partner Banking Framework Services reassessment has commenced and is expected to be completed by early July, and a number of low risk product re-assessments are currently overdue. However, two new Financial Crime Managers join the team at the end of June which will ensure that remaining outstanding re-assessments can be brought up to date by the autumn. All new product and service assessment and support is being completed.

Supply Chain Compliance

37. One audit was completed in May and 3 Improvement Needs were identified, with an audit score of 5 which is in line with the national average. Two further audits were completed in June but at the time of

POL00423568

writing this paper, the reports had not been finalised. No significant or recurring issue identified.

Financial Services

Credit Cards

38. The Marketing Services Agreement (which has Compliance requirements) and the Appointed Representative Agreement (ARA) is close to agreement with Capital One. This will also entail changes to the existing ARAs with BoI as well as a new multi principal agreement (MPA) between all the Principals. The MPA is to ensure that boundaries of regulatory responsibility are clear between Principals and are largely dividing responsibility along product lines.
39. Any new Principal agreement needs to be consistent with the approach taken with our existing regulatory Principals to ensure consistency of application and purpose. Following the agreement on the ARA we will need to put in place a Regulator Guidance Manual that outlines the key responsibilities PO has to put in place to maintain compliance. We also need to agree financial promotions and sales material approval processes with Capital One.

Current Account Withdrawal

40. We are monitoring this with BoI, there are 21,500 current account customers and as at the end of May:
    - 3,181 customers have switched their accounts to another provider
    - 3,927 customers have closed their accounts
    - 7,108 customers in total which is 33% of the all customers

41. Around 1,000 customers have withdrawn the majority of their money through an ATM and these customers will be asked if they would like assistance closing through a bespoke mailing.

42. There were 50 complaints last month regarding delays in the closure process. BOI have conducted root cause analysis and identified incorrect details provided by customers on forms, delays in authenticating customers for higher value transactions and stretched resources in their closure department as key constraints.

43. Customers taking action from the most recent mailing has not been as high as expected. There is a more direct mailing scheduled for early July and PO will seek to understand BoI plans to ensure we are comfortable that we get as many customers as possible to take action whilst protecting customers and our brand.

Mystery Shopping Results

44. Branch Mystery Shopping results for May show poor conformance to the Travel Insurance sales process, where colleagues are not giving the Eligibility and Medical Laminate to customers so they can confirm medical condition status. Training is being provided in Q2 to align with the summer

POL00423568

45. Video Mystery Shopping results have dipped since April when we had no reds to 8 reds in May, 4 Savings and 4 Life Insurance. The decline can be attributed to the restructure and re-focus of the Area Manager team with less time available for support of CRMs. Communication is ongoing with the CRM and lead teams.

Network Management changes

46. We are working with the Network teams on the changes they are making to their branch management approach, including CRMs. The aim being to maintain appropriate oversight and conduct management but to reduce the burden on the network teams. We are under particular pressure particularly from BoI to ensure we articulate our proposed controls.

Vulnerable Customers

47. The Vulnerable Customer Module and test was launched on Success Factors on the 20th May. A wider network awareness initiative was supported by Network Team Talks and awareness packs for Area Managers to brief Postmasters. This was preceded with a talk on the Alzheimer's Friends initiative at Finsbury Dials led by the Graduates and the NFSP.

48. An external accessibility expert Kate Nash Associates has completed the review of our PO Vulnerable Customer Policy. This has concluded that it meets all the requirements expected. She is proposing some introductions with leading firms in the vulnerability space, including Barclays and Sainsbury's on how they meet vulnerability challenges and ideas on how we can further improve.

Citizens' Advice (CA) Super Complaints to Competition and Markets Authority (CMA) relating to the 'loyalty penalty'

49. The Secertary of State for BEIS wrote to the Chief Executive of the CMA on 19th June strongly supporting the findings of the super complaint (reported at previous Committee).

50. The Government has already committed to legislate in order to give consumer enforcers the power to impose fines on companies for breaches of consumer law by applying to the courts.

51. BEIS propose to follow this through empowering the CMA to decide for itself whether consumer protection law has been broken and then impose fines for wrongdoing directly. CMA will consult on how best to achieve this although it would be a surprising outcome if it decided to intervene in areas already regulated by Ofcom and FCA.

52. BEIS also announced on 17th June a related Smart Data Consultation. The paper sees huge potential for data-driven services (smart data) to enter consumer markets and stimulate competition. BEIS want consumer markets in the UK to be at the forefront of the Artificial Intelligence (AI) and data sharing revolution.

POL00423568

53. There are potentially significant issues mainly for Telco which we are assessing and will respond if appropriate by 6th August.

54. This includes a proposal that Ofcom supported by new legislation, should lead the implementation of Open Communications requiring communications providers to share customer and product data to aid switching.

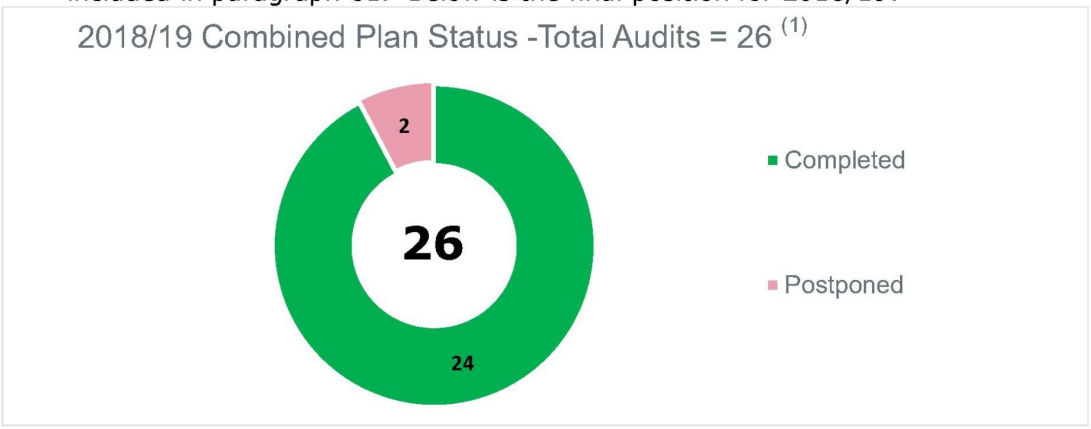
55. For the Financial Services Areas impacted by the super complaint, (mortgages, cash savings and general insurance). There has been no further substantive news since the last Committee although updates are expected sometime this year.

Internal Audit

Author: Johann Appel

Progress against plan (2018/19)

56. We have delivered 24 of the 26 reviews on the 2018/19 internal audit programme. The remaining two reviews are change assurance reviews, which were delayed due to the change portfolio being reprioritised. These two programmes have been included in the 2019/20 change assurance plan.
57. Seven reviews have been finalised since the May ARC, with summaries included in paragraph 61. Below is the final position for 2018/19:

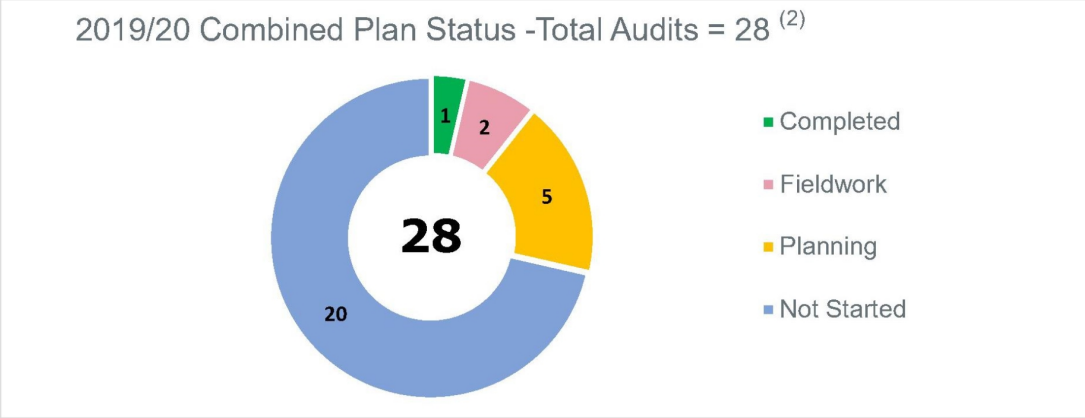


(1)ARC approved baseline plan for 2018/19 (16 core internal audit reviews & 10 change assurance reviews). A full summary of the 2018/19 audit plan status is included in appendix 6.

POL00423568

Progress against plan (2019/20)

58. We have finalised one review, with a further 2 in fieldwork and 5 being planned for delivery in Q2:



(2)ARC approved baseline plan for 2019/20 (18 core internal audit reviews & 10 change assurance reviews). A full summary of the 2019/20 audit plan status is included in appendix 6.

Reporting on Control Themes for 2018/19

59. In 2018/19 Internal Audit raised a total of 271 audit actions to remediate identified control weaknesses (2017/18 = 165). All internal audit findings were analysed to identify recurring control themes and root causes. The top four control themes were as follows, with full results included in Appendix 7.

Control Theme	18/19	17/18	
Internal controls are not deployed through policies, procedures and systems and/or internal controls are not designed or operating effectively.	36%	40%	↓
Ineffective identification and/or management of operational, fraud and change risk (including unclear expression of risk appetite).	8%	13%	↓
Unavailability (or ineffective communication) of relevant, quality information to support the internal control function and decision making.	17%	10%	↑
Lack of clarity of structure, authority and responsibility.	12%	10%	↑

POL00423568

Report turnaround

60. In May 2017 the ARC requested an internal service level agreement for clearing of audit reports. The target was set at 20 working days (10 days for Internal Audit to produce a draft report and 10 days for management to review and comment). Actual time to clear audit reports has been considerably more and has further deteriorated in 2018/19.

61. Average report turnaround in working days was as follows:

	18/19	**17/18**	
IA to prepare draft report (target = 10 days)	16	15	↑
Management to review and comment (target = 10 days)	25	21	↑
Total (target = 20 days)	**41**	**36**	↑

62. We have taken steps to make the report clearance process more effective. This includes the introduction of formal audit close meetings with both operational management and the executive sponsor. In addition, the Interim Chief Executive has established a clear escalation process to help address any significant delays. Our co-source auditors have agreed to the new process and we have the full support of the GE to improve the report turnaround.

6

POL00423568

Internal Audit reviews in progress and planned for delivery in Q2

63. The following reviews are being planned for delivery in Q2 (A full summary of the 2019/20 audit plan status is included in appendix 6):

	Review	Status	Timing
1	Procure to Pay	Fieldwork	24/06 – 19/07
2	Data Analytics Excellence (Change)	Fieldwork	12/06 – 28/06
3	Effectiveness of Gating – Design Effectiveness (Change)	Planning	08/07 – 26/07
4	Effectiveness of Second Line Assurance – Design Effectiveness (Change)	Planning	08/07 – 26/07
5	Benefits Realisation – Design Effectiveness (Change)	Planning	08/07 – 26/07
6	Investment Funding Follow-up (Change)	Planning	August
7	Payment Technology Upgrade (Change)	Planning	Sept
8	Telco Billing Process	Planning	July
9	Employee Expenses Follow-up	Planning	August
10	Payzone Internal Controls 'Health Check'	Planning	August
11	POI – Change Capacity	Planning	July
12	POI – AR Oversight (Operating Effectiveness)	Fieldwork	17/06 – 05/07
13	POI – Nemesis Follow-up	Planning	August

Status of Audit Actions

64. A total of 271 audit action were raised in 2018/19 (2017/18 = 165). During the same period management completed 163 audit actions (2017/18 = 134). Audit actions are generally being completed on time. As at 26 June 2019 there were 106 open actions, 4 of which were overdue.

Audit Action Status:	
Open (not yet due)	102
Overdue (<60 days)	4
Overdue (>60 days)	0
Total	106

Changes to plan since March ARC meeting

65. There were no changes made to the 2019/20 audit plan, which was approved at the March ARC meeting and is included in appendix 6.

POL00423568

Internal audit reviews completed

66. Since the May ARC meeting we have finalised the following eight reviews:

- Contract Management (IT)
- IT Control Framework
- Payroll
- Payzone Integration (Panther)
- Change Excellence (Follow-up)
- P2C Belfast Exit
- FS Training
- Pensions Follow-up (2019/20 plan)

Our findings and observations from these reviews are summarised below, with the full reports circulated to the committee separately:

Payroll Process (Ref. 2018/19-18)



Sponsor:
Mo Kang

Audit actions:

P1	1
P2	8
P3	0
Total	9

Payroll processing was found to be effective and well managed, however, the audit has identified some shortcomings that require remediation. Key findings are:

The Payroll team spend a considerable amount of time correcting poorly submitted payroll data on behalf of the business units, which adversely impacts their core processing work. The current level of overpayments to employees due to late or incorrect submissions of data (annualised at approximately £240k) is largely avoidable. Line managers will be reminded of their responsibility to submit timely and accurate payroll data to enable the payroll to be processed efficiently.

There is inadequate segregation of duties, which are partly caused by the overlapping of role based permissions. This could be efficiently and securely addressed by introducing a supervisory level between the Payroll manager and the Payroll assistants.

There is a lack of visibility of configuration changes by Accenture and inappropriate access to the file transfer server (SFTP) where the BACS payment files are saved. These weaknesses, combined with limited reconciliation of BACS payments and reconciliation issues between SuccessFactors and CFS give rise to a risk of inappropriate payments being made.

Despite the control deficiencies noted above, we highlight that the risk was mitigated by effective compensating controls and no irregularities were identified during the audit. This conclusion was confirmed by the application of extensive data analytics, which enabled us to provide assurance, with a high level of confidence, over the completeness, validity and integrity of the payroll, and the quality of data, over the 12 months sampled.

Management Comment provided by Mo Kang

"Firstly, thank you to the Audit team for their collaborative and supportive way in which they have continued to work with the team and help improve our ways of working, processes and systems. The is the first payroll audit that has been carried out since the implementation of Success Factors and the audit has highlighted some areas which we need to address, which the team were largely

POL00423568

aware of and have been working on, particularly the education of line managers and the role they play across all the processes which impact on payroll, how and when data needs to be submitted to the HRSC and we will continue to educate and support our line managers. This will be addressed through holding open day surgeries to help educate and upskill line managers, which the Systems Team will carry out in Bolton, Chesterfield and Finsbury Dials. The Business Partnering function will also continue to support line managers and use their monthly operational meetings to address and educate the business on Success Factors.

The HRSC is already on a journey to codify, simplify and automate processes and implementing these actions will help us towards achieving that. There has been considerable progress made since the implementation of Success Factors and the team have learned how to operate the system effectively as they have progressed. There are still controls to be refined and issues to be addressed but there are agreed actions to ensure these are covered off."

IT Contract Management (Ref. 2018/19-15)



Needs Improvement

Sponsor:
Rob Houghton

Audit actions:

P1	1
P2	6
P3	5
Total	12

This internal audit was done at the request of IT management, following an independent maturity assessment performed by ISG in Q1 2018. The audit assessed the progress made since the 2018 review and will also inform a review of Post Office wide contract management processes, which is planned for 2020/21.

We conclude that the IT Contract Management (CM) team is in the process of embedding a number of positive changes with examples of good practice and mature processes observed. We highlight that the strategic direction taken and the actions set following the ISG review in Q1 2018, are driving significant improvement in the operating effectiveness of the contract management processes and its maturity as operated by the IT CM team. Some recommendations were made to further enhance IT CM processes and maturity.

The review highlighted the lack of a Post Office wide owner at GE level for the contract management process. There is also no overarching contract management policy and controls framework on which processes and minimum controls are established. This is key to enable effective and consistent management of CVM activities within a defined minimum requirements framework and a defined risk appetite.

Management Comment provided by Catherine Hamilton

"The CM team has demonstrated its significantly increased maturity and the discipline and rigour demanded by the large and complex contracts that collectively deliver technology to Post Office. The P2 and P3 actions identified by IA will further enhance our processes and maturity. To address the P1 action across Post Office, I am preparing a proposal for the COO and General Counsel to extend the discipline and best practice across Post Office, with outcomes including a documented Contract Management Policy and Strategy, Supplier Tiering standards, Community of Practice and Governance standards."

POL00423568

IT Control Framework (Ref. 2018/19-24)



Sponsor:
Rob Houghton

Audit actions:

P1	0
P2	6
P3	3
Total	9

Post Office has established an IT Controls Framework (ITCF) based on ISACA's COBIT 5 model. The framework has been live since January 2018, with multiple processes added in December 2018.

The introduction of the ITCF was a fundamental step in providing management with the ability to identify and address control deficiencies effectively. Our review confirmed that the framework is generally operating effectively, however, we recommend that the ITCF be enhanced by:

- Introducing a formal activity to develop and refine processes and controls.
- Improving understanding of the ITCF through enhanced communications and training.
- Implementing a more fully featured tool to support the ITCF.
- Developing management information to provide improved feedback to senior management, process owners and control owners.
- Defining roles and responsibilities for ITCF governance and assurance.

Management Comment provided by Catherine Hamilton

"The ITCF has been shown to be operating effectively with clear opportunities to further optimise and increase maturity over time. We will assess the technology and consider whether any further investment will enhance our ability to identify and measure IT operational risk."

6

POL00423568

Payzone Integration (Change Assurance Review) (Ref. 2018/19-29)



Sponsor:
Debbie Smith

Audit actions:

P1	1
P2	6
P3	0
Total	7

The shortcomings noted in this audit are balanced by observations of good practice as well as management and workstreams leads' commitment and strategic focus on the delivery of the business case, which reduced the risk and limited the impact on the business. Observations were separated between pre- and post-acquisition activities:

Pre-acquisition: We noted that management has adopted a pragmatic approach towards the delivery of the Payzone acquisition and has sought external support when needed. This enabled a successful completion following CMA approval and a smooth day one transition. However, we have observed some weaknesses in the pre-acquisition activities and integration planning that should be recorded as lessons to be learned for future M&A activities. Specifically:

- An upfront, clearly defined scope and well-articulated set of questions to be answered during due diligence.
- Greater formalisation and clarity over roles and responsibilities.
- The completion of a thorough assessment and prioritisation of the tasks to be completed in the first 100 days post acquisition, tailoring to Post Office needs and business priorities, as to drive an integrated Day 1-100 execution.

Post-acquisition: Shortcomings in the Day 1-100 plan (being only a subset of all transition activities), combined with insufficient resource planning, resulted in the plan not achieving its objectives. The plan was not appropriately re-assessed in light of scope, strategy and priority changes, and as knowledge of the acquired business increased. The pursuit of commercial opportunities and remediation of issues noted post-acquisition also added pressure on the delivery of the plan and the activities directly driven by the workstream leads.

As such full execution of the plan has been delayed with 460 of the planned 1,056 activities not being completed. Failure to adequately execute the key transition activities may lead to an overall erosion of the business case (by adding costs and elongating the time to integrate Payzone). Management has concurred with our view that a comprehensive re-plan and re-prioritisation exercise should be completed in light of the transition activities pending completion. The outcome of this work should be a standard 'Day 100+ Second Wave' Post-Merger Integration (PMI) process, consolidating the tasks from the Day 1-100 plan still outstanding, TSA exit and the wider integration activities.

We have also noted weaknesses in governance arrangements, monitoring of progress with integration activities and mechanisms to track benefits – these are now being addressed.

Management Comment provided by Andrew Goddard

We found this audit to reflect a fair and reasonable assessment of the pre and post-acquisition activity. There are a series of valuable learnings and improvements for future acquisitions, specifically in the due diligence, planning, and resourcing of an M&A structure. There are also a range of valuable recommendations to manage through the Second Wave plan of work. We have already actioned a series of these by disbanding the PMO in favour of an internal programme team to re-calibrate the separation, integration, and business as usual workload in a more compact and integrated team structure. This will enhance the reporting and overall governance."

POL00423568

Belfast Exit (Change Assurance Review) (Ref. 2018/19-27)



Sponsor:
Rob Houghton

Audit actions:

P1	0
P2	6
P3	3
Total	9

The Belfast Exit programme aims to migrate Horizon from the Belfast data centres (managed by Fujitsu) onto a Fujitsu managed cloud platform, hosted in Microsoft's Azure.

We found the programme set-up and delivery processes to be broadly appropriate with evidence of good practice across the scope areas reviewed. An area particularly strong was the management of Fujitsu with the team adopting an active pragmatic approach and addressing issues by working collaboratively and following Agile principles.

The review highlighted some areas of improvement, most notably a requirement to re-assess the Data Privacy Impact Assessment (DPIA); inaccuracies or uncertainties in the migration cost estimates; and a need to improve communication of the change freezes and its impacts across Post Office.

The programme carried a high inherent risk, being a complex migration; involving Post Office's crown system, Horizon; and competing both in terms of time and resources with other Post Office key initiatives, particularly in Retail.

As we finalised this audit report, we were made aware of the decision to pause and postpone the migration for twelve months. The decision, while allowing the business to focus on other significant initiatives and address risks with the migration plan, also allows management more time to address observations from this audit.

Management Comment provided by Rob Houghton

"The decision to defer the transfer of Horizon into cloud was made due to change window impact, impact on Horizon specialist skills and the benefit of a longer time window to mitigate migration risks before a major operational risk of an Horizon move. This timing enables the resolution of the findings of the audit report as the remediation actions will be built into the revised timeline. Accordingly the paper is for noting and I would propose that the actions and rating are postponed and the programme is re-audited upon re-initiation."

POL00423568

Change Excellence Follow-up (Change Assurance) (Ref. 2018/19-26)



Sponsor:
Rob Houghton

Audit actions:

P1	0
P2	4
P3	2
Total	6

The Change Excellence programme (CEX) (previously Project Trafalgar) aims to enhance Post Office's Change delivery capabilities.

CEX was divided into four Programme Increments (PI), implementing incremental capabilities to increase Change maturity from 1 out of 5, as assessed at the start of the programme to a target maturity of 3. Our review assessed the effectiveness of the processes, controls and governance as it delivers these programme increments. We also assessed progress with actions from the previous CEX advisory review.

The programme believes that PO's Change maturity has increased to a level of 2.5 at the end of PI3. Whilst we have not performed a formal maturity assessment, the audit has found that significant progress was made. However, we noted areas of improvement and work still outstanding and highlight that governance needs to be improved, particularly:

- SPO's mandate is not clear. At present it does not enable in full the driving of the implementation and bedding-in of delivery processes and the incremental improvements.
- SPO also needs to agree with GE the sanctions for not delivering in accordance with the revised framework.
- Greater clarity is needed in regards to the roles of the Design Authority (DA), Enterprise Architecture Group (EAG) and the Change Approvals Group (CAG).

The revised governance is key to assist with bedding in of key capabilities, controls, and tools deployed, including Service Now (SNOW), Anaplan, SAP Project Accounting, and the Competency Framework, and to continue to drive a shift to Agile principles (70% of programmes are still waterfall in nature). While finalising this review, we were made aware of imminent governance changes driven by the McKinsey report. As these are not yet final and formally communicated across Post Office, we have maintained the detailed observations as-is and will (when appropriate) amend the agreed actions in line with the pending changes.

Management Comment provided by Kevin McKay

"We note the recognition of improvement in change process and tooling and accept that there remains further work to ensure these improvements are embedded so as to deliver the outcome of improved change delivery performance. Whilst we have sought to trial SAFe Agile from a tooling perspective, which we completed in March, we have not yet trialled SAFe at a portfolio level across Post Office which is anticipated to require some organisational change. This is intended to be part of the Organisational Effectiveness work originating from the McKinsey Blueprint. The Design Authority forum has been reviewed and merged with CAG to form the Portfolio Review Board, starting mid-May. Other items identified here are in hand though not all being addressed by Change Excellence Programme."

6

POL00423568

FS Training (Branch Sales) (Ref. 2018/19-04)



Sponsor:
Debbie Smith/ Owen Woodley

Audit actions:

P1	0
P2	1
P3	1
Total	3

POL has a regulatory responsibility, via its AR agreements, to put effective systems and controls in place by which colleagues involved in the introduction and sale of POL's FS products receive appropriate training and oversight.

POL maintains governance mechanisms to align its training obligations and objectives with those of its Principals. Governance committees are properly set up and operate effectively, providing forums for approval, challenge and escalation of FS training and related matters.

The rollout of Smart IDs represents a move towards a system-based preventative approach to controlling the delivery, completion and monitoring of training activities across the network, and early indications are that it is working well and delivering the expected benefits. This change, combined with the removal of higher risk product sales such as mortgages from branches, has enabled POL to streamline its approach to training into two streams (for CRMs and non-CRMs), which are well understood across the business functions that contribute to training delivery. We note that there is no overall documented training policy, the existence of which would allow POL to easily demonstrate to stakeholders that the current approach to training is appropriate and would provide a clear benchmark against which future reviews and refreshes can be made. We recommend that action is taken to capture the overall approach.

Management Comment provided by Cathy Mayor

"We take POLs responsibilities as an AR very seriously and are therefore pleased to be rated Green, Satisfactory. The two improvements recommended will be implemented before the end of September 2019"

6

POL00423568

Pensions Process (Follow-up review) (Ref. 2019/20-01)



Sponsor:
Mo Kang

Audit actions:

P1	0
P2	3
P3	3
Total	6

The 2018/19 audit concluded that controls over the Pensions process needed significant improvement. Management agreed to implement a total of 23 remedial actions.

The Audit, Risk and Compliance Committee (ARC) requested that Internal Audit perform a follow-up audit to validate the implementation status of the 23 actions raised in the 2018/19 audit.

Salary sacrifice was introduced in November 2018 which led to process changes. Management asked us to review this area more broadly, in addition to following up on the prior year audit.

Since the last audit the management of the pension scheme and collaboration across both the Pensions and HRSC teams is much improved. There were no regulatory issues or control failures identified and the salary sacrifice scheme is working as intended.

The work done by both the interim team in London and the Payroll team in HRSC has seen the number of reportable errors significantly reduced.

Management Comment provided by Mo Kang

"The findings of the audit compared to the previous pensions audit in September 2018 are a significant marked improvement in what has been a relatively short period of time, a fantastic achievement and thankyou to the Audit Team for their support throughout this piece of work. The HR target Operating Model implementation, changes of personnel within the Reward team and the teams working much closer together have been significant enablers for the HR function overall.

Further improvements are being made within our processes and systems, regularly reviewing our ways of working and establishing the Pensions Governance meetings with the HRSC, Reward Team, AON & Scottish Widows are evidence of the progress and achievements made.

However, I acknowledge & understand that there is more work to do on how our payroll team is structured in the HRSC to align with our operational needs, role based permissions and segregation of duties and plans to address this issue are being developed by the HRSC.

In summary, great progress has been made and I have every confidence that we will continue to build on this with the right people, structure, skills and experience in place within the function."

POL00423568

Appendix 1. Risk Heatmap

Principal Risks	Trend / Risk Green Status Expected Date	Retail	FS&T, Identity and POI	CFO-Finance	Ops (COO)	LCG	CIO incl CISO,IT<BCP,BPA	HR (incl. H&S)	COMM	ALL	July-'19 Comments
Operational	May-'19	↑				↓	↔			n/a	**Red** - There is one ongoing red risk relating to cheque clearance process. Work continues on mitigations through negotiations with BoI and longer term the plan is to move Cheque Deposit envelopes for PO Money deposits. **Key amber points** - The Safety Compliance Top Risk remains 'Amber' as improvements to H&S training and compliance remains ongoing, including developing guidance for Agents. In COO work continues to improve support to agents balancing and resolving pay queries. IT experienced a couple of major incidents in June (Agents payroll and loss of MS Teams and Office 365) all issues resolved promptly.
	Jul-'19	↔								n/a	
Information Security	May-'19									n/a	**Red** – Whilst Info Security is not called out as red, Cyber Threat will remain a focus area and forms part of our top-risk profile. Update from CISO in RCC pack. **Key amber points** - For LCG are reviewing resourcing for DP activities. Work is continuing on GDPR and data processes to ensure compliance and effective management.
	Jul-'19									n/a	
Technology	May-'19		↑				↑			n/a	**Red** - No business area is currently reporting high concerns. **Key amber points** – Work is underway to assess whether the Fujitsu campus failover should take place at the end of August. A risk workshop has been arranged with key stakeholders to ensure the risks are identified and mitigated appropriately. Additionally Verizon have postponed 9 scheduled DR tests to date. This has been escalated within Verizon, Vendor Management and the service team. It is a concern that the tests will not be performed within the agreed 12 month period.
	Jul-'19		↔				↔			n/a	
Third Party	May-'19						↑				**Red** - For LCG, Contract Mgt and Poor Contract Design remain an ongoing focus. Work to remediate has been primarily around the high value contracts. A new procurement tool will help fix, which is currently being procured and due to be in place by Nov 2020. **Key amber points** – No new issues called out.
	Jul-'19									n/a	
Legal & Regulatory	May-'19	Re. PCI ↑	↑			Re. PCI ↑	Re. PCI ↑			n/a	**Red** – PCI remains a key concern (RCC pack confirms latest position). CISO reports two red risks relating to insider threat and failure to include security and data privacy controls in contracts with suppliers. Work is underway to remediate which include; training, L&D programmes, and controls implemented via the JML programme. For Retail the Top risk around Cash Withdrawal Card transactions – update is within the risk. Telco have identified and are working on potential changes required to meet the requirements for PSDII and the full outcome of the text relay issues is outstanding. Update expected by the end of June. **Key amber points** - No new issues called out.
	Jul-'19	Re. PCI ↑	↔			Re: Litigation	Re. PCI ↑			n/a	
	Green status Expected Date	Nov-20				Nov-20	Nov-20				
Financial	May-'19									n/a	**Red** - There is a key risk over Ofcom pricing differential review that remains a concern. This is focused on the over 65s, which accounts as a large volume of the POs customer base. Commercially we have decided to take a reactive approach to this. An update from Ofcom is expected in September 2019. **Key amber points** – For LCG 'Demand Management' is being rolled out to improve forecasting. Ops loss prevention team is now in place and continues to work on process improvements.
	Jul-'19									n/a	
Strategic	May-'19									Brexit	**Red** – No new red risks. Retail Proposition and Brexit remain and updates are within the Top Risk Profile. **Key amber points** - Identity remains Amber, however has moved to a worsening position as the increasing potential of competitive forces in the market has started to grow. Our plans could be stifled if the major banks/ tech start-ups move into this space.
	Jul-'19									Brexit	
	Green Status Expected Date	Oct-19	Oct-19							Oct-19	
People	May-'19		↑							n/a	**Red** - The digital competency people risk which remains rated as Red (building teams with right skills and capabilities) has been redefined as Talent Acquisition. **Key amber points** - There are several risks around the lack of resource support the Back office Transformation and Cloud enablement both with the Service area, the risks are within appetite as a result of colleagues within IT supporting the low resourced areas.
	Jul-'19		↔							n/a	
Change	May-'19								n/a		The overall status of the portfolio continues to be Amber. Refer to main body of the report.
	Jul-'19								n/a		

↓ Improving ↑ Worsening ↔ Stable

6

POL00423568

Appendix 2: Top Group Risks (Included in the reading room)

Appendix 3: Metrics reviewed for Multiple Partners

Commercial Partner
Listed
Exchange
Market Cap (£)
Current Share Price (£)
Share price high (LTM)(£)
Share price low (LTM) (£)
Share price % change (LTM)
Share price % change (L3M)
S&P Long-Term Company Rating
S&P Outlook/Credit Watch
Stock on loan %
Net Debt/EBITDA
Total Debt/Equity
Interest cover (Earnings/int.exp)
Recent Announcements/upcoming events
Comments

Finance (RAG)
Number of Company operated POs within estate
Number of Symbol operated Pos within estate
Total of whole estate
Acquisitions Company operated (LTM)
Disposals Company operated (LTM)
Disposals of PO with retail retained CO (LTM)
Remuneration (£) YTD
Remuneration variance YoY (%)
Reported PO P&L (if applicable)
Additional supporting information
Relationship Manager Feedback
CEO Feedback (date)
Notes
Post Office (RAG)

6

POL00423568

Appendix 4: Change Portfolio: Gold & Platinum programme/projects dashboard[1]

	Project Name	Investment Type	RAG Statuses				
			Cost RAG	Benefits RAG	Delivery RAG	Risk RAG	Overall RAG
F&O	Back Office Transformation Programme	Service Sustaining	Amber	Green	Amber	Amber	Amber
F&O	Data & Analytics Excellence - DAE (Arrow)	Strategic Enabler	Amber	Amber	Amber	Red	Amber
F&O	Future of Stock	Cost Reduction	Green	Green	Green	Green	Green
F&O	Post Office Business Opportunity-Agent On boarding	End User Experience	Green	Green	Green	Amber	Amber
F&O	Process & Contact Centre	Cost Reduction	Amber	Amber	Green	Green	Green
F&O	Self Service Portal (Branch Hub)	Cost Reduction	Green	Amber	Green	Green	Green
F&O	Source to Settle	Cost Reduction	Green	Amber	Green	Green	Green
F&O	SF EUM Common services	Strategic Enabler	Green	Green	Green	Amber	Green
F&ST	Home Phone and Broadband Nuance	Cost Avoidance	Green	Green	Green	Green	Green
HR	Blueprint	Cost Reduction	Green	Green	Amber	Green	Amber
HR	Success Factors - Phase 2	Strategic Enabler	Amber	Green	Amber	Green	Amber
Identity Services	IDS Digital Identity	Strategic Enabler	Green	Green	Amber	Amber	Amber
IT & Change	Belfast Exit	Cost Reduction	Green	Green	Green	Green	Green
IT & Change	PCI Compliance	Legal and Regulatory	Red	Amber	Red	Red	Red
IT & Change	Advanced Security Operations	Strategic Enabler	Green	Green	Green	Green	Green
IT & Change	Project Everest	Legal and Regulatory	Green	Amber	Green	Green	Amber
LRG	General Data Protection Regulation	Legal and Regulatory	Green	Green	Green	Green	Green
LRG	Legal Entity Optimisation - LEO	Strategic Enabler	Amber	Green	Red	Red	Red
LRG	Fit and Proper	Legal and Regulatory	Amber	Amber	Amber	Amber	Amber
POI	Home Insurance Transformation (POI – Nemesis)	Strategic Enabler	Green	Green	Amber	Green	Amber
POI	Home & Travel Insurance Pricing & Data Analytics (POI – Morpheus)	Strategic Enabler	Green	Green	Green	Green	Green
Retail	Digitising Mails	Revenue Protection	Green	Green	Green	Amber	Amber
Retail	Horizon Integration Hub	Strategic Enabler	Green	Green	Green	Green	Green
Retail	Automated Locals	Revenue Generating	Green	Green	Green	Green	Green
Retail	Cheque Image In-clearing and Out-clearing	Legal and Regulatory	Green	Green	Amber	Amber	Amber
Retail	Enhanced User Management	Legal and Regulatory	Green	Green	Green	Green	Green
Retail	Future of POca	Revenue Generating	Green	Green	Amber	Green	Amber
Retail	Network Development	Service Sustaining	Green	Green	Green	Amber	Green
Retail	Parcel Shop	Revenue Generating	Green	Green	Amber	Amber	Amber
Retail	POca Implementation 17/18	Service Sustaining	Amber	Green	Red	Amber	Red
Retail	SSK Procurement	Cost Avoidance	Green	Green	Amber	Amber	Amber
Retail	SSK Simplification	End User Experience	Green	Green	Green	Green	Green
Retail	SSK Trial	Strategic Enabler	Green	Green	Green	Green	Green

[1] Data taken from Strategic Portfolio Office Change Monthly Executive Summary (P2) – June 2019

POL00423568

Appendix 5: Compliance Status Heat map

Sector	Current Assessment	Previous Assessment	Comment/Action
Telecoms Compliance			Ofcom has confirmed it is to investigate the Text Relay issue and we are supporting it with its information requests. We have signalled that we are open to exploring an early settlement, which was proposed by the regulator may be offered
Data Protection			The status has reverted to Amber due to the remedial work identified through the GDPR Gap analysis. A separate paper outlining action steps and timeframes is being presented to the RCC for consideration.
AML/CTF			We have received annual invoice from HMRC for £3.2m and have raised with BEIS but it is likely Post Office will have to pay this invoice. Progress is being made collecting the agents fit and proper data, but there are issues with resolving partial/non-responses
Whistleblowing			No material issues to report. See separate annual Whistleblowing report and policy review.
Anti-Bribery and Corruption			No material issues to report. See separate ABC annual policy review and report
Supply Chain Compliance			14 improvement needs from 4 audits in the 3 months to April. No material issues - satisfactory overall
Financial Services Compliance and Conduct Risk			We are working with PO Money on strategic product change initiatives for credit card new providers and current account closure. This includes new Appointed Representative agreement and management of new regulatory Principal. Status has moved to Amber due to the instances of non-conformance identified through mystery shopping.
Vulnerable Customers			Alternative format literature provision-we are currently at the final stage of contract negotiation with an external provider. When complete this metric should move to green (expected end July)
Policy Governance		n/a	Policy governance and accountabilities are being reviewed and effective controls established.

6

KEY:

	Material items of concern that require focussed remediation to ensure we stay within our risk appetite
	Some items of concern that could breach appetite if they crystallise or are not managed
	Within overall appetite

POL00423568

Appendix 6: Internal Audit Plan Status

2018/19 Internal Audit Plan – Re-prioritised (ARC approved 30 Oct 2018) - Status at 26 June 2019					
No.	**Title/Subject**	**Sponsor**	**Original / Addition**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	Product Risk Review (Postal Orders)	O. Woodley	Original	April	Needs Improvement
2	Employee Expenses	A. Cameron / M. Kang	Original	April	Unacceptable
3	Procurement Fraud Investigation	A. Cameron	Addition	May	Not Rated
4	Month-end Close Process	A. Cameron	Addition	Nov	Satisfactory
5	MoneyGram Compliance	O. Woodley	Addition	Sept	Satisfactory
6	Contract Management (IT)	R. Houghton	Original	Oct	Needs Improvement
7	Whistle-blower Process	J. MacLeod	Original	Oct	Satisfactory
8	Opening of Bank Accounts	A. Cameron	Addition	Nov	Satisfactory
9	FS Training & Competence	O. Woodley	Original	May	Needs Improvement
10	Cyber Security	R. Houghton	Original	Jan	Not Rated
11	IT Control Framework	R. Houghton	Original	March	Needs Improvement
12	Financial Control Framework	A. Cameron	Original	Jan	Needs Improvement
13	Payroll	M. Kang	Original	Feb	Needs Improvement
14	Client Settlements Process	A. Cameron	Original	Jan	Satisfactory
15	Agents Remuneration	A. Cameron	Original	Jan	Needs Improvement
16	Network and SGEI Reporting	D. Smith	Addition	Feb	Needs Improvement
17	Procure to Pay	A. Cameron	Original	Q4 / Q1	Postpone[2]
18	Branch Cash Forecasting & Management	A. Cameron	Original	Q1 19/20	Postpone[1]
19	Supply Chain Management	A. Cameron	Original	Q1 19/20	Postpone[1]
20	Digital Strategy & Capability	O. Woodley	Original	2019/20	Postpone[2]
21	Online Sales	O. Woodley	Original	2019/20	Postpone[2]
22	Data Privacy (GDPR Follow-up)	J. MacLeod	Addition	Q1 19/20	Postpone[2]
Change Assurance[3]					
1	Change Excellence (Trafalgar)	R. Houghton	Governance	May	Advisory Report
2	DMB Strategy	D. Smith	Programme	July	Satisfactory
3	Branch Hub (Agents Portal)	D. Smith	Programme	October	Needs Improvement
4	Investment Funding Controls	R. Houghton	Governance	November	Needs Improvement
5	Payzone Integration (Panther)	D. Smith	Programme	Jan	Needs Improvement
6	Digital Identity Services	M. Edwards	Programme	Feb	Needs Improvement
7	Change Excellence (Follow-up)	R. Houghton	Governance	March	Needs Improvement
8	P2C Belfast Exit	R. Houghton	Programme	March	Needs Improvement
9	Digitising Mails	D. Smith	Programme	TBC	Postponed to 19/20
10	Payment Technology Upgrade (PCI)	D. Smith	Programme	TBC	Postponed to 19/20

[1] Delay until after BOT programme is complete and new controls embedded.

[2] Postpone due to process still bedding down and maturing (GDPR) / restructuring (Digital & Online) / remediation (P2P).

6

POL00423568

[3]The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2018/19 at the time. The list is being reviewed and updated on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum' projects.

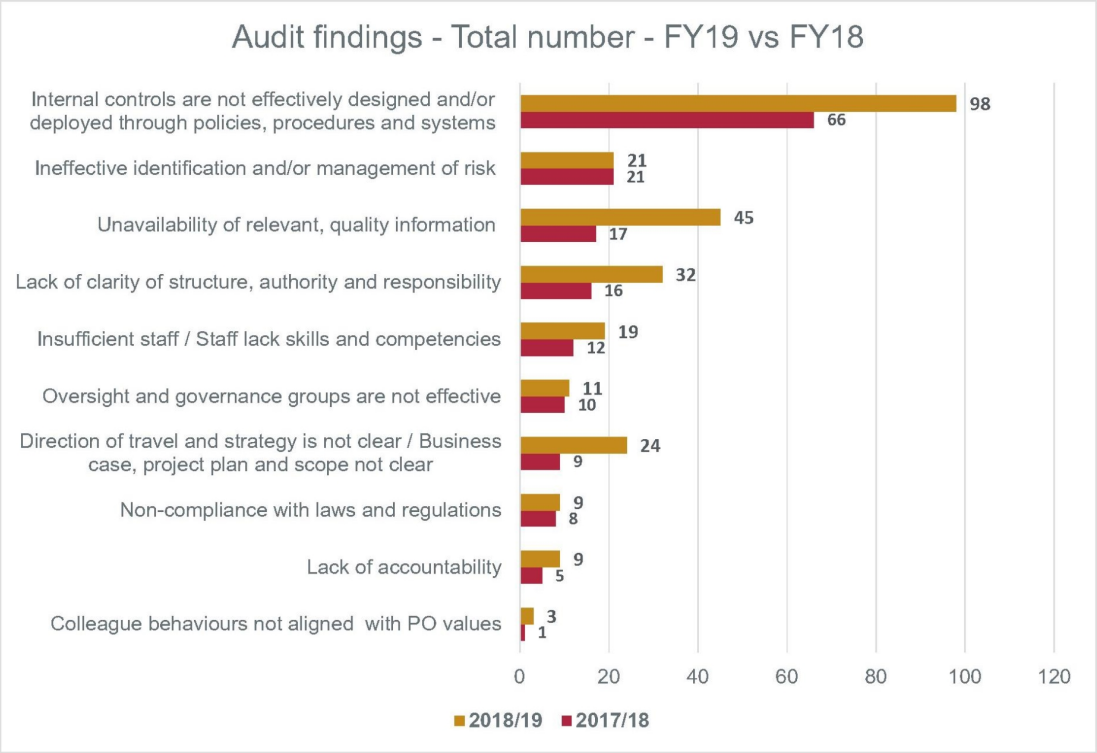
2019/20 Internal Audit Plan - Status as at 26 June 2019					
No.	**Title/Subject**	**Sponsor**	**Source**	**Timing**	**Status / Rating**
Internal Control Reviews					
1	Procure to Pay	Interim CFO	Original	June	**Fieldwork**
2	Branch Cash Forecasting	Rob Houghton	Original	Aug	Not started
3	Supply Chain (CViT)	Rob Houghton	Original	Aug	Not started
4	Accounts Receivable	Interim CFO	Original	Flex	Not started
5	Agent On-boarding	Debbie Smith & Rob Houghton	Original	Q4	Not started
6	Pensions Follow-up	Mo Kang	Original	May	**Satisfactory**
7	Employee Expenses Follow-up	Mo Kang	Original	August	**Planning**
8	Branch Banking Framework	Debbie Smith	Original	Q3	Not started
9	Sales (Savings Accounts)	Owen Woodley	Original	Q3	Not started
10	Vetting / Fit & Proper	Ben Foat & Rob Houghton	Original	Flex	Not started
11	Effectiveness of Risk Management Framework	Interim CFO	Original	Flex	Not started
12	CFS Controls (Post BOT)	Interim CFO	Original	Q2	Not started
13	Effectiveness of Compliance Function	Ben Foat	Original	Flex	Not started
14	Telecoms Customer Billing	Owen Woodley	Original	July	**Planning**
15	Data Privacy (incl. follow-up of GDPR)	Ben Foat	Original	Q4	Not started
16	Cyber Security Follow-up	Rob Houghton	Original	Q2	Not started
17	Payzone Control Framework	Debbie Smith	Original	Q2	**Planning**
18	FS Branch Sales	Owen Woodley & Debbie Smith	Original	Flex	Not started
Change Assurance[1]					
1	Investment Funding Controls follow-up	Rob Houghton	Governance	Jul / Aug	Not started
2	Effectiveness of 2nd line Programme Assurance	Interim CFO	Governance	July	Not started
3	Benefits Realisation (Product Realisation)	Rob Houghton	Governance	July	Not started
4	Portfolio Level Operational effectiveness (excl. assurance, and gating process)	Rob Houghton	Governance	tbd	Not started
5	Effectiveness of the Gating Process	Rob Houghton	Governance	July	**Planning**
6	Belfast Exit (phase 2)	Rob Houghton	Programme	Sept	Not started
7	Data Analytics Excellence	Rob Houghton	Programme	June	**Fieldwork**
8	PTU (PCI Compliance)	Rob Houghton	Programme	September	**Planning**
9	Digitising Mails	Debbie Smith	Governance	tbd	Not started
10	Identity Services (Follow-up)	Owen Woodley	Programme	tbd	Not started

[1]The list of Change Assurance reviews was approved by the ARC on the basis of being the highest risk programmes planned for 2019/20 at the time. The list is being reviewed and updated on an ongoing basis to reflect the programmes most deserving of independent assurance, predominantly 'Platinum' projects.

6

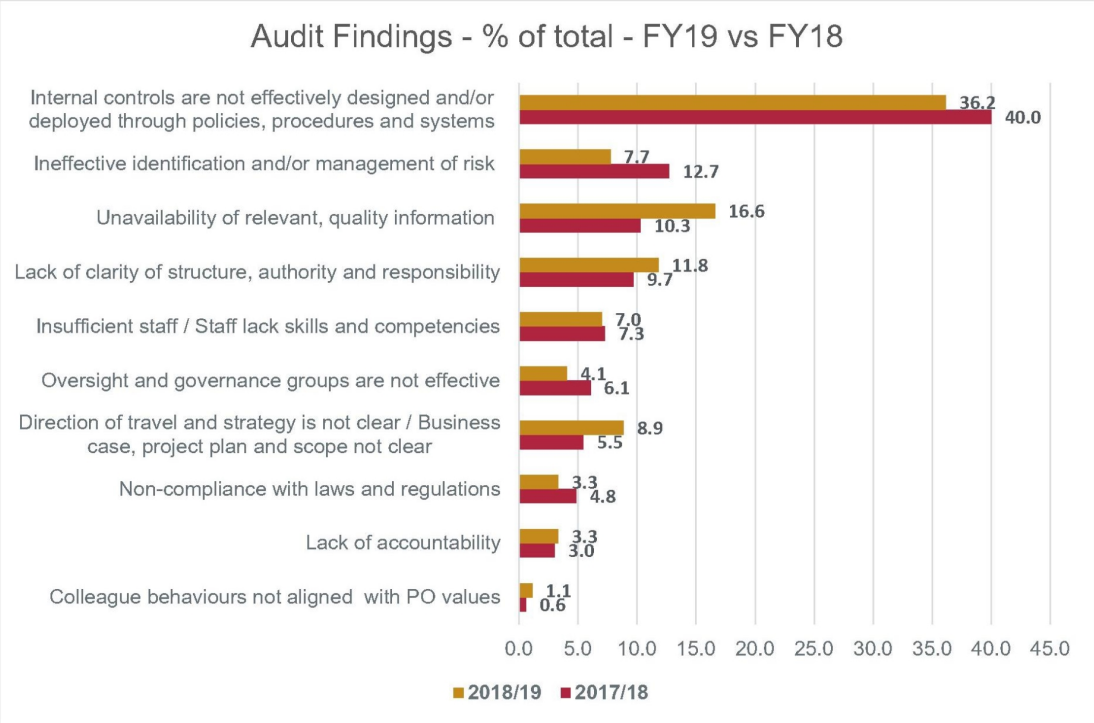
POL00423568

Appendix 7: Audit findings mapped against COSO control principles (N1)



6

POL00423568



Commentary:

- The percentage of audit findings relating to ineffective control activities has reduced by almost 4 percentage points, indicating that operational controls are improving / maturing.
- Likewise, risk management appears to be more effective, with findings reducing by 5 percentage points.
- However, there appears to be a deterioration in the control components 'control environment' and 'information & communication', as the number of findings around availability of information, clarity of structure and direction of travel (unclear strategy) have in total increased by almost 12 percentage points.

6

POL00423568

Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework mapped to Post Office control themes

Control Component	Control Principles	Post Office Audit Themes / Root Cause
Control environment	1. Demonstrate commitment to integrity and ethical values	1. Colleague behaviours not aligned with PO values
	2. Exercise oversights responsibilities	
	3. Establish structure, authority and responsibility	2. Lack of clarity of structure, authority and responsibility
	4. Demonstrate commitment to competence	3. Insufficient staff / Staff lack skills and competencies (Insufficient training and commitment to continuous development of colleagues)
	5. Enforce accountability	4. Accountability is not enforced; management style does not encourage a culture of being accountable
Risk assessment	6. Specific suitable objectives	5. Direction of travel and strategy is not clear
	7. Identifies and analyses risks	6. Ineffective identification and/or management of operational, fraud and change risk (this could include unclear expression of risk appetite)
	8. Assesses fraud risk	
	9. Identifies and analyses significant change	
Control activities	10. Selects and develops control activities	7. Internal controls are not effectively deployed through policies, procedures and systems and/or internal controls are not designed or operating effectively. Includes lack of up to date process documentation.
	11. Selects and develops general controls over technology	8. Non-compliance with laws and regulations.
	12. Deploys through policies and procedures	
Information and communication	13. Uses relevant information	9. Unavailability of relevant, quality information to support the internal control function and decision making (or ineffective communication of such information)
	14. Communicates internally	
	15. Communicates externally	
Monitoring activities	16. Conducts ongoing and/or separate evaluators	10. Oversight and governance groups are not effective in identifying and correcting control weaknesses.
	17. Evaluates and communicates deficiencies	

(N1) COSO has established a common internal control model against which companies and organisations may assess their control systems. The COSO control model is underwritten by the Institute of Internal Auditors. The above table shows how the Post Office control themes map to COSO control components and principles.

6

POL00423568

6.2 Procurement Compliance Reporting

Author: Barbara Brannon Sponsor: Al Cameron Meeting Date: 4 July 019

Executive Summary

Context

As a business in receipt of public funds POL is bound by the Public Contract Regulations (2015). PCR 2015 oblige POL to behave in a fair, objective & transparent way when contracting with 3rd party suppliers. Additionally, set procedures must be followed for spend above £25k and £181,302.

Failure to abide by the legislation or "slicing and dicing" contracts exposes POL to risk, both as far the commercial outcomes of the contracts as well as the reputational damage, legal remedies, censure & fines that can follow the discovery of a breach. Our compliance to PCR can be requested under a Freedom of Information request at any time.

The PCR Compliance Register allows for the tracking of breaches to PCR regulations at the Post Office and internal governance processes. One aim of collating this information is to drive improvement in awareness and compliance behaviour across the organisation. The second and primary aim is to work with GE and Business Units to commence commercial reviews in a more timely way ensuring POL obtains value, commercial and contractual flexibility fitting the requirements and business strategy of the organisation.

Questions addressed in this paper

1. *How many and what types of procurement non-compliance have occurred in the past quarter?*
   Since the last RCC report in January there have been a total of 37 non-compliant PCR incidents with a total value of **IRRELEVANT**
   A list of these awards is set out at the end of Appendix A.

2. *What are we doing about it?*

POL00423568

Active reviews continue with Business Units with the highest values relating to non-compliance. A number of tenders with material values attached were completed on schedule by the financial year end.

Approved business strategies and therefore associated Sourcing [buying] activities and associated timetables to resolve non-compliance within Identity Services and, Brands/Rapp are outstanding.

Our overall non-compliance value has dropped slightly from IRRELEVANT in January to IRRELEVANT

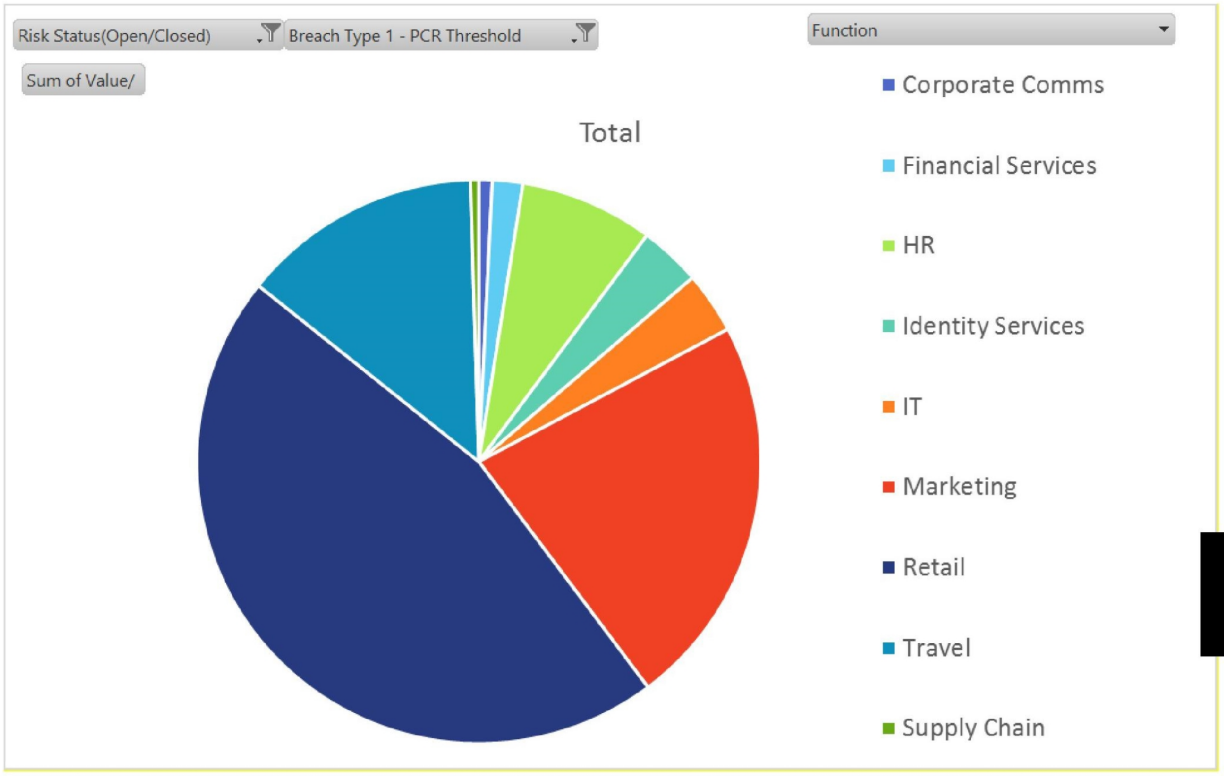
This was primarily driven by closure of some material risks through compliant procurement awards and contracts reaching a statute of limitation on a challenge period. New risks of IRRELEVANT for Marketing [aggregated] and £10m for Globalpay were entered into between January 2018 and July 2019.

Open non-compliant awards since January **2017** are outlined below and a detailed list of high value open items is within Appendix B.

Non Compliance Value by Business Function.

	Jan-19	Jul-19		
Function	**Sum of Value**	**Sum of Value**	**Variance**	**Comment**
Corporate Comms	IRRELEVANT			New direct award for GLO. Legacy risks closed
Financial Services				Customer Hub Support + misc small contracts
HR				Successfactors, SAP, Recruitment [partial]
IT				SSK Support & Service Now
Marketing				Brands, Ensighten, Caci, Aggregator renewals
Retail				
Network				
Travel				Award Pending in August
Identity Services				Digi-identity
Retail				Globalpay, Oliver Wyman, Egremont, Smith & Ouzman
Supply Chain				
Post Office Insurance				
Grand Total				

POL00423568



7

3. What is in the current Procurement pipeline which is high value and at risk of being awarded or extended non-compliantly?

Update on previously advised:

a) £10m pa. A 1yr extension for our Payments provider to complete a technology upgrade programme with the business actively working on its replacement strategy has been completed,

b) £1.2m pa. Successfactors – Enterprise HR software system SaaS contract renewal. Paper submitted to GE, December 2018. Non-compliant 12 month renewal executed April 2019, paying for only what we use. This has taken our SF costs from a budgeted £1.2m in 2018/19 to £539k in 2019/20 a saving of £711k. Work will commence in July to identify route to compliance/replacement when new G-Cloud framework is published.

c) £800k. SSK support with NCR for 2019 pending an agreed sourcing solution. Business requirements not ready for market as yet. Discussions and quote processes ongoing with IT suppliers on required software development.

d) £1m Brands/Rapp – this has been extended again in April 2019. A business strategy, funding and sourcing plan needs to be agreed.

POL00423568

Discussions are continuing with Marketing and IT on their key upcoming renewals to identify the sourcing options which are appropriate for the required operating models/cost drivers/business strategy.

An agreed strategy to bring POL recruitment services/agencies into compliance is outstanding along with Staff and Agent Vetting, the latter moving to Network Operations but with continuing HR requirements to be built in. HR have appointed a Recruitment Manager who is working with Procurement to update options presented in 2018. As recruitment budgets are decentralised, a briefing paper will be prepared by HR and Procurement for GE and L40 for discussion.

Conclusion

Non-compliant awards of contracts are already subject to extensive internal governance, legal and risk review, in line with POL governance guidance on value and risk.

Individually, all large value non-compliant contracts have been reviewed by appropriate Post Office governance forums with agreement on next steps and actions towards remediation allocated where appropriate.

Executive support towards moving POL towards a more compliant footing is very strong, but equally as important there is extensive support towards the cultural change required to ensure that Procurement activities and outcomes will support longer term business strategies and we reduce commercial risk making our 3rd party arrangements fit for purpose.

Input Sought

None – for discussion and further action if required.

POL00423568

Appendix A

1. What are the potential consequences of non-compliant awards?
   a) Pre-contractual remedies overview: During a Procurement, an aggrieved party can seek an interim injunction suspending the tender or the implementation until the court decides on an outcome.
   b) Post-contractual remedies: The court can order an 'ineffectiveness order' rendering the contract void &/or can award damages.

2. Why are these incidents of non-compliance occurring, and what can be done about it?

   Non-compliant awards are made for a variety of reasons at the Post Office.

   a) Low value, time constrained or highly sensitive/specialist engagements are common. For example, a number of expedited reviews since the New Year on a short turn-around time.
   b) Large commercial arrangements cannot often be easily competed or unravelled without operational impact, and re-procurement may be subject to a pending evolution of a supporting Business Strategy.
   c) The contractual arrangements may pre-date PCR 2015 regulations or the contract novated during separation from RMG, automatically becoming non-compliant at the renewal point. Non-compliant awards are frequently made on a tactical basis to extend contractual services while public tender processes are executed.
   d) Delays to public sector panels of suppliers becoming available. The Post office makes extensive use of this low cost route to market and new/refreshed panels are subject to frequent delays from Crown Commercial Services. Single interim extensions [of periods under 12 months] while tender processes are run are considered to be low risk legally.
   e) Changes in scope or value over the term of a contract may render the extension or renewal of services non-compliant. Material changes to the scope of a contract may render the whole contract non-compliant.
   f) Disregard for, or lack of understanding of the regulations.

3. Why are we receiving this report?

   A decision to collate this information into a single location was taken in the Autumn of 2016. The aim is to track and improve our overall compliance and commercial results as an organisation, while also ensuring perceptions are accurate. However it should be noted that it will facilitate timely responses to

POL00423568

Freedom of Information requests which adds risk to the Post Office commercial landscape.

4. Are any of these breaches arguable on regulatory grounds or are they all breaches?

   A full explanation of the individual compliance breaches for direct awards over £181k [previously £164k] threshold is attached in Appendix A. Each entry details the nature of, and the value of the breach. The threshold is altered annually based on the FX rate between GBP and the Euro.

   The Procurement Compliance Register does not at present give an indicative risk level attached to the award. This information is provided to the accountable executives under internal governance processes in the form of a PCR risk note before a contract above threshold is entered into, and if necessary under Legal Privilege. In addition, all signatories to a contract have sight of the Risk note as part of the Contract Authorisation Form [CAF].

   All entries are compliance breaches. A period of challenge applies to each PCR breach once an aggrieved party becomes aware or ought to have become aware. This risk finally expires at 6 years from the date of breach. The defensibility of a legal challenge is outlined within a Risk Note.

5. *How many of the breaches were approved in advance and how many retrospectively?*

   All contracts entered into during this period were compliant with internal governance processes on contract and commercial review. All were for awards of between £0 and £4,000,000 with the exception of the Globalpay extension which was the subject of a Board report.

6. *Why were the approvals given?*

   The rationale for approval is relevant to the individual service and is detailed within Appendix A.

7. *What were the unapproved, material breaches?*

   There were no unapproved, material breaches during this period.

8. *Describe what you are doing about the breaches. Where we are in breach, do we have a plan to come back into compliance and over what time period will that plan take effect?*

a) A forward view of material contracts falling under each Business Unit is currently prepared by the relevant Procurement Manager for discussions with

POL00423568

their key stakeholders. The maturity of this look ahead view does vary currently and is consistently a high priority activity within the team.

b) Sourcing options papers are prepared for review by contract managers and key stakeholders [risk, legal, security] with routes to market agreed. In many cases these are dependent on evolving business and operating model strategies and the Procurement team are now actively involved with some units helping to advise and review options as thinking evolves.
c) Where a non-compliant award is proposed due to time pressure, Procurement are actively working on long term mitigation with awards made on an interim basis to meet urgent operational needs.
d) Each RCC member now receives a regular report on compliance within their business unit[s].
e) A new Risk & Governance process requires a Risk Exception report to be created for non-compliant direct awards with SLT or GE sign off.
f) All Professional Services engagements must be approved in writing in advance by the COO. A compliant panel of preferred consulting partners has been appointed and proposed engagements outside of this panel are subject to additional review and challenge.
g) Procurement provides training as part of the revised Induction process for new staff. Training packs are being updated for existing staff and a new training module made available on Successfactors. Ad hoc training sessions for interested Business Units are also run.
h) A new Intranet site has been launched for Procurement to improve visibility of process, regulation, and the panels of approved compliant suppliers available to POL business units.
i) A revised POL Procurement Policy and supporting processes is in progress giving more granular guidance.
j) Using Crown Commercial Services frameworks, panels of Preferred Suppliers are being refreshed and updated across a wide range of spend categories to reduce time to market, improve compliance and greatly improve commercial outcomes and legal risk.
k) A planned change to operational systems will, once live, give Procurement earlier visibility of potential compliance issues eg: contractual value thresholds.

POL00423568

New Incidents [PCR & Internal Governance] over Reporting Period - Open Risks only.

New Incident	Date	Procurement Category	Function	GE Member	SLT (GE-1) person	User / Staff Name	Supplier Name	Value/ Income
1	29/01/2019	Management consultancy	Retail	Debbie Smith	Tom Moran	John Dineen	IRRELEVANT	
2	28/02/2019	Creative Services	HR	Jo Arakji		Emma Campbell		
3	28/02/2019	Marketing	Marketing	Owen Woodley	Emma Springham	Piers Langendon		
4	28/02/2019	Marketing	Financial Services	Owen Woodley	Chrysanthy Pispinis	Frankie Arnull		
5	01/03/2019	Goods for Resale	Retail	Debbie Smith	Andrew Goddard	Nick Spicer		
6	01/03/2019	Marketing	PO Insurance (no PCR)	Owen Woodley	Russ Taverner	Paul Dashwood		
7	04/03/2019	Creative Services	Finance	Alistair Cambell		Steph Ball		
8	05/03/2019	Marketing	Marketing	Debbie Smith	Katharine Challinor	Steve Kirby		
9	14/03/2019	Marketing	Marketing	Owen Woodley	Emma Springham	Piers Langendoen		
10	23/03/2019	Marketing	Marketing	Owen Woodley	Henk Van Hulle	Sephora Jenks		
11	25/03/2019	Professional Services	Retail	Debbie Smith	Mark Siviter	Lindsay Allan		
12	25/03/2019	Recruitment & Agency	Retail	Debbie Smith	Roger Gale	Lindsay Allan		
13	26/03/2019	Recruitment & Agency	HR	Mo Kang	Emma Campbell			
14	26/03/2019	Recruitment & Agency	HR	Mo Kang	Steve o Reilly			
15	26/03/2019	Professional Services	Finance	Alistair Cameron	John Flood			
16	27/03/2019	Goods for Resale	Retail	Debbie Smith	Mark Siviter	Laura.A.Plunkett		
17	04/08/2019	Recruitment & Agency	Financial Services	Owen Woodley	Sean Leahy	Sean Leahy		
18	10/04/2019	IT SaaS	HR	Mo Kang	Rob Houghton			
19	22/05/2019	IT SaaS	Marketing	Owen Woodley	Henkvan Hulle	Neil McDonald		
20	23/05/2019	PR	Marketing	Owen Woodley	Joanne Leahy	Caroline Keany		
21	23/05/2019	Courses	Retail	Debbie Smith	Pamela Heap			
22	23/05/2019	Telecoms	PO Telecoms (no PCR)	Owen Woodley	Meredith sharples	Matt Keeffe		
23	23/05/2019	Public Affairs	Corporate Comms	Mark Davies	Patrick Bourne			
24	23/05/2019	PR	Marketing	Owen Woodley		Caroline Keany		
25	23/05/2019	Marketing	Marketing	Owen Woodley	Mic di Stazio			
26	23/05/2019	Recruitment & Agency	Marketing	Owen Woodley	Henk Van Hulle	Bella Slade		
27	04/06/2019	IT Hardware	Supply Chain	Alistair Cameron	Andrew Preston	Darren Mullen		
28	13/06/2019	Coaching/mentoring	Corporate Comms	Mark Davies	Jane Hill	Alistair Cameron		
29	13/06/2019	Recruitment & Agency	HR	Mo Kang	Sean Leahy	Sean Leahy		
30	13/06/2019	Recruitment & Agency	HR	Mo Kang	Caroline O Donnell	Caroline O Donnell		
31	13/06/2019	Recruitment & Agency	HR	Mo Kang	Caroline O Donnell	Caroline O Donnell		
32	13/06/2019	Cash Handling	IT	Rob Houghton	John Flood	John Flood		
33	15/06/2019	Marketing	Marketing	Owen Woodley	Emma Springham	Grant Ballie		
34	15/06/2019		Retail	Debbie Smith				

7

POL00423568

Appendix B

Date	Procurement Category	Function	GE Member	Supplier Name	Value/ Income	Rationale for Non Compliant Extension Approval
23/03/2017	Professional Services	HR	Mo Kang	IRRELEVANT		
10/01/2018	Travel	Travel	Alisdair Cameron			
10/01/2018	Professional Services	HR	Mo Kang			
10/01/2018	IT Software	IT	Rob Houghton			
15/02/2017	Comms, R&I & PR	Corporate Comms	Mark Davies			
04/07/2018	IT Software	Marketing	Owen Woodley			
04/07/2018	IT Software	Retail	Debbie Smith			
28/08/2018	Marketing	Retail	Debbie Smith			
	Professional Services	Retail	Debbie Smith			

POL00423568

Appendix B

04/01/2019	Goods for Resale	Financial Services	Owen Woodley
29/01/2019	Management consultancy	Retail	Debbie Smith
28/02/2019	Marketing	Marketing	Owen Woodley
01/03/2019	Goods for Resale	Retail	Debbie Smith
14/03/2019	Marketing	Marketing	Owen Woodley
10/04/2019	IT SaaS	HR	Mo Kang
22/05/2019	IT SaaS	Marketing	Owen Woodley
23/05/2019	Marketing	Marketing	Owen Woodley
15/06/2019	Marketing	Marketing	Owen Woodley
15/06/2019		Retail	Debbie Smith

IRRELEVANT

POL00423568

Resilience, Business Continuity & Crisis Management update

Author: Tim Armit Sponsor: Tony Jowett Meeting date: July 2019

Executive Summary

Context

Operational Resilience and Business Continuity is in place across key areas which meets business requirements. The 2018 audit report of business continuity capability identified gaps in the documentation and governance which needed to be addressed. This paper reports on progress against the audit findings and the current resilience and continuity position across Post Office.

There is a need to sign off the Business Continuity Policy annually which is due now.

Risks this paper addresses

- The progress against the business continuity audit report of December 2018.
- The status of resilience and business continuity across Post Office.
- The requirement for annual sign off of the Business Continuity Policy.

8.1

Input Sought

The Committee is requested to sign off the policy and note the report.

Conclusion

1. Audit responses are on schedule. This report focusses on responses for December 2018, earlier responses were reported to RCC and ARC on time in 2018.
2. The attached Risk Appetite report covers the Risk Appetite for Business Continuity across Post Office and the Strategies adopted for resilience and business continuity.
3. The attached Business Continuity Policy requires sign off.

POL00423568

The Report

What is the status of progress against the audit report findings due in December2018?

- The business continuity audit report found "a lack of strategic plan and consideration of risk appetite for BCM".
- To demonstrate progress against the audit report the attached document presents the Business Continuity Risk Appetite. This details the appetite for all key areas where continuity and resilience solutions are implemented across Post Office. The report focusses on:
  - Locations
  - Systems
  - Business Functions
  - Suppliers
- The risk appetite document has been created following interviews and reviews across all areas. It has been validated by key business areas and there is some work ongoing, some areas are shown red as we do not have a confirmed position.
- IT have their own controls in place for Disaster Recovery of systems and their own compliance measures. The appetite shown in the Business Continuity document is that of the business to the loss of systems.
- Contractual requirements are key in confirming the appetites ensuring Post Office recovery requirement meet contractual agreements. This review is ongoing across all business areas. Work continues to identify who owns and is responsible for each contract to ensure business areas take full responsibility.
- The risk appetite report attached presents the appetite for all areas and the current situation for each area and how confident Post Office should be that the strategies in place meet the appetites requirements.
- From the report a plan will now be developed that allocates owners and people to action to reduce the level of exposure from unknown or red.
- The report will continue to grow as more business functions and suppliers are brought on board and as levels of resilience improve thus reducing the exposure.

What is the status of resilience and business continuity across Post Office?

1. Background - In 2016 Post Office had no planned recovery capability for its key locations or operations. It had a dysfunctional response to crisis and escalation with no clear reporting lines. There were no documented impacts of a failure and no plans per business area to be used in an incident. The historic Royal Mail group documentation in place across Supply Chain had become unfit for purpose. Controlled and manageable communication to staff and branches had not been possible.
2. Current position – The table below shows the current status across Post Office with regards to crisis communication and business continuity capability.

   It is key that all staff can be communicated with in and out of working hours and that we can track staff safety in an evacuation. Post Office now has that capability in key offices and operations.

   Post Office has never had the capability to simply communicate to all branches in the event of a Horizon failure and a solution for this has now been implemented.

   Business continuity recovery strategies are now in place and tested for all location incidents.

POL00423568

3. Communication Status

Area	Capability	Status
Finsbury Dials	650 people via Grapevine single text blast	Tested
Chesterfield	350 people via Grapevine single text blast	Tested
Business Protection Team	all areas via Grapevine single test blast	Tested
GE Gold Team	all areas via Grapevine single test blast	Tested
Supply Chain	all depots, cash centres and trucks via Grapevine single text blast	Tested
Branches	every branch via Grapevine single text blast	Tested

4. Business Continuity Status

Location	Plans	Impacts	Strategy	Status
Finsbury Dials	In place	Known	Work from home	Tested
Chesterfield	In place	Known	Sungard Site	Tested
Bolton	In place	Known	Sungard Site	Tested
Bristol	In place	Known	Sungard Site	Tested
Supply Chain	In place	Known	Mutual Support	BAU
Swindon	In place	Known	Swansea	IT tested
IT systems	In place	Known	DR solutions	Partially tested

- Resilience in building design is being improved across key locations and resilience in contracts and IT is under constant review.
- Business Continuity is now established, embedded and moving from a development and implementation stage to a business as usual state that can be easily maintained and monitored. This changes the status of the role going forward.
- Future Challenges –The scope of business continuity covers all risks that may impact the reputation, income, customer service and operational capability of Post Office. As such all risks must be robustly challenged to ensure management have considered them and have responses in hand should they unfold. Areas being challenged:
    a. Horizon failure across all branches for an extended period
    b. Brexit
    c. Political changes to Post Office and its operations including its role as a bank
    d. Succession planning and key role risks

POL00423568

e. On-boarding new companies and roles of directors
f. Horizon trial and contingency responses
g. Risks of success across business functions
h. Cyber risks and the changes as we go forward

POL00423568

Business Continuity Risk Appetite

8.1

Author Tim Armit
Date June 2019
Version 0.1

POL00423568

Introduction

This report details the risk appetite within the Post Office business areas for the loss of key business locations, functions, systems and suppliers.

It considers the "pain" the business would suffer if each of these areas was impacted by an incident and identifies when this would become intolerable.

The report is divided into four sections:

1. An overview of the approach, the terms used and the assumptions that were used.

2. The risk appetite for key areas currently included within the business continuity programme.

3. Areas and risks which are not currently at a level that meets the desired risk appetite and a work status of the current strategies in place and assesses the adequacy of these to meet the desired appetite. This enables the reader to focus on only the key risks to Post Office.

4. Areas and risks which currently meet the desired risk appetite and presents how this is achieved and any further work that is required to continually improve this.

Assumptions:

1. A systems analysis review was completed across the business and IT in 2017 which identified the key IT systems and the required recovery times the business needed for these. This report identified Horizon and the networks as the only critical system within Post Office at that time. The impact of all other systems being down can be mitigated for two days with minimal affect.

2. The report focusses on business operations and appetite is considered from this standpoint. The business continuity and resilience team focusses on maintaining business services as such all assumptions are with this in mind.

3. It is acknowledge that with change and development this report will have to continually develop and change. Currently not in the report but being challenged for inclusion are:

   - The digital CDP layer
   - Branch finder
   - Apps (Travel, Customer Hub)
   - IT Self service
   - Parcel Shop
   - Fujitsu homephone and broadband

POL00423568

Appetite Summary

The over arching simplistic assumption on risk appetite that underpins business continuity is that if the branches are open and the customers are being served then Post Office is operational.

All other services which underpin the business and keep it functioning are seen as secondary if the primary objective is achieved.

The table below details the risk appetite for each key aspect of Post Office operations. The scope covers all aspects of Post Office for which continuity solutions are considered and will be updated and amended as the scope changes.

Areas considered within the report (the lists within these tables will continue to grow as more detail is gleaned during the work programmes):

Locations	Key locations which support Post Office operations directly. Most are within the direct control of Post Office some are covered by contracts. The dependency on the location and the resilience in design and recovery capability in place are all considered.
Systems	Key IT systems which support business operations are considered in terms of their significance and the disaster recovery solutions in place.
Business Functions	Key business functions which deliver or support Post Office operations.
Suppliers	External suppliers which deliver key services to support Post Office operations.

Risk Appetite is measured as:

Appetite	Impact and Tolerance	Requirement
Averse	Post Office has a low level of tolerance to any impact or outage. A solution to maintain the service is required.	1 day recovery or less
Neutral	Post Office can tolerate some downtime and the outage has tolerable impact. A solution is required but a longer period to recover is acceptable.	2 to 4 days recovery
Tolerant	Post Office can tolerate the service being non operational for an extended period of time with minimal impact.	Over 4 day's recovery.

Strategy Status is measured as:

Summary	Definition
Green	A solution is in place, it has been tested and meets business needs.
Amber	A solution has been identified that meets business needs but has not been tested.
Red	No solution is in place

POL00423568

Business Continuity Risk Appetite Where Strategy Status is Red

The table below details the risk appetite for each key aspect of Post Office operations which do not have resilience or continuity solutions in place that would meet business needs in a crisis. The scope covers all aspects of Post Office for which continuity solutions are considered and will be updated and amended as the scope changes. This report is a live document and is ongoing as work is completed in areas and as areas are strengthened with solutions implemented and tested.

Risk Appetite Tables

Locations	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Payzone Data Centres	Averse	Loss of Payzone operations	Resilient design across two data centres.	Moving data centres to increase resilience. Planning in place to move to an outsourced provider and infrastructure requirements will form part of this move.	Red
Swindon	Neutral	Loss of stock supply to branches	Alternate warehouse provision and systems	Swansea identified as potential recovery area but not tested, systems to be made resilient and recovery proven. Systems are green but building is red (no business continuity)	Red

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
NONE RED					

POL00423568

The Systems table appetite is the impact on the business not on IT operations and as such there is work required to ensure the IT assumptions align with the business needs.

IT have confirmed there is a varying level of disaster recovery testing in place across all suppliers and a regular monthly review of progress. BC team is working with IT on the detailed level of this and how it meets business needs. This item will be broken down into each supplier as the information is confirmed.

Systems	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Verizon	Averse	Loss of all branch operations. Loss of all other business operations.	Zero down time	TBC. Many failures with Verizon across 2018 which have stablised recently. IT to confirm the resilience in the Verizon network for continual service and to confirm the disaster recovery time should key component areas of Verizon be lost.	Red
Call Centre ACD/IVR	Averse	Loss of ability to manage calls to NBSC	2 hour recovery time	TBC. Will be picked up in the Verizon / Puzzel resilience review.	Red
Call Centre systems (Dynamics)	Averse	Loss of ability to respond in a coordinated manner to incoming NBSC calls	2 hour recovery time	TBC. Working with NBSC and IT to confirm.	Red
Fujitsu Belfast Horizon	Averse	Loss of Key critical IT systems including Horizon, MDM, Credence	Resilient design with zero down time and disaster recovery solutions	Full datacentre test has not been carried out for five years. Secondary datacentre is within the same region. Horizon branch data base has been successfully recovered in an alternative datacentre. Component tests of systems have been carried out successfully. MDM and Credence have been switched to an alternate site. Site is an N+1 site. There is a contracted 2 hour recovery time for POCA / Banking / Vocalink and debit card payments which can be met. All other Horizon services are contracted for a 5 hour recovery. Moving some to the Cloud which will improve resilience but not change contractual recovery times. Work to be done with IT to confirm each Data Centre has resilience in its design (infrastructure, power etc). The exit from Belfast will improve the levels resilience levels.	Red
APOP	Neutral	Loss of payments out system	Recovery within 2 working days	The system remains a stand PC in Chesterfield.	Red

POL00423568

The supplier risk is the risk of a supplier failing that provides services to Post Office business areas.

The levels business continuity capability within suppliers own operations are key to Post Office. Post Office needs to know that services and operations completed by suppliers can be continued should a supplier suffer a major incident. This has not been challenged before and is now being completed. Most large organisations will have proven continuity in place, but Post Office is not currently aware of this, as such suppliers are in the main shown as amber / red but will be changed as responses are received. Requests for this information are with suppliers.

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Fujitsu	Averse	Unable to deliver system support to Post Office systems	Zero down time	TBC.	Amber / Red
Computacenter	Averse	Unable to deliver system support to Post Office systems	Zero down time	TBC.	Amber / Red
ATOS	Averse	Unable to deliver system support to Post Office systems	Zero down time	TBC.	Amber / Red
Accenture	Averse	Unable to deliver system support to Post Office systems	Zero down time	TBC.	Amber / Red
Ingenico	Averse	Unable to process card payments	2 hour recovery time	The Contract states there is recovery capability in place but further evidence that this meets business needs is required.	Amber / Red
Grapevine	Averse	Unable to provide security support for branches. Unable to support all crisis response tools in place for Post Office. Unable to support evacuation process. Unable to communicate to all branches.	Zero down time, resilient systems, alternative office space.	Page One (underlying system) failed in late 2018 and was down for over 2 hours which presented a problem to Post Office. Other resilience is in place but further testing of the systems is required. Working with Grapevine to liaise with Page One over resilience levels.	Red

POL00423568

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
CBRE	Averse	Unable to respond to building issues	Intra day recovery times	TBC working with facilities team	TBC
Servest	Averse	Unable to support the management of key locations	Intra day recovery times	TBC working with facilities team	TBC
Banks	Neutral	Unable to deliver support to operations externally to support the Banking Framework	Intra day recovery times	IRRELEVANT	Amber / Red

POL00423568

Business Continuity Risk Appetite Where Strategy Status is Green / Amber

Risk Appetite Table

Locations	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
POMS Glasgow	Averse	Loss of Insurance call centre support	Recovery Office	Webhelp have plans in place, and tested, to restore the call centre at their alternative offices. This works well unless there is extreme weather in Scotland and they are all closed, as happened last time it was needed. POI have accepted this risk.	Green
Preston Call Centre	Averse	Loss of POCA call centre support	Recovery Office	Plans and strategy in place, annual testing takes place	Green
Supply Chain Depots	Averse	Loss of depot or cash centre, loss of supply or collection of cash to branches.	Alternate depots and cash centre processing equipment	Resilient depots and identified third party depots. This is amber due to no physical testing of the capability to stand up Hemel spare machines or testing of how the two main cash centres would support each other.	Amber
Payzone Offices	Averse	Loss of Call Centre and head office functions	Recovery Office	Agreement to share old Payzone offices for a period of time. Planning in place to implement a Sungard solution to meet business needs and to increase the operational resilience within the office.	Amber
Chesterfield	Averse	Loss of Branch support Call Centre, Treasury and Finance Service Centre	Recovery Office	Sungard solution in place and tested	Green
Bristol	Averse	Loss of cash ordering process	Recovery Office	Sungard solution in place and tested	Green
Computacenter DC	Averse	Loss of key systems	Resilient design with zero down time and disaster recovery solutions	Full datacentre test run in 2018 successfully. Regular and ongoing component tests undertaken.	Green
Accenture DC	Averse	Loss of key systems	Resilient design with zero down time and disaster recovery solutions	Datacentre test run in 2017 successfully. Regular and ongoing component tests undertaken.	Green
Verizon DC	Averse	Loss of network and Puzzel ACD IVR Call Centre systems	Resilient design with zero down time and disaster recovery solutions	Datacentre test run in 2017 successfully. Regular and ongoing component tests undertaken.	Green
Finsbury Dials	Tolerant	Loss of head office functions and strategic leadership	Home working capability and recovery office	Home working solution proven and Sungard solution in place.	Green / Amber
Bolton	Tolerant	Loss of internal human resources support services	Recovery Office	Sungard solution in place and tested	Green

POL00423568

Key central systems have a 4 hour contracted recovery time which is required to be tested annually. Manual work arounds are in place and proven for all key systems except Horizon.

Systems	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
CFS	Averse	Loss of systems to support the finance operation and the supply chain operation.	4 hour recovery time	CFS is in Azure. It moved recently so although Azure tested last year with Credence/MDM (Sept 18) it hasn't been tested with the new systems in it. A test is proposed for the beginning of Sept. The recovery time (RTO) Is 4 hours as per the SLA.	Amber
Email	Neutral	Loss of key communication tool.	Intra day recovery time	Technology is in place to provide robust email. Use of webmail in extremis is possible. Testing of this has not been undertaken. Mimecast can deliver a solution to this and testing of this should be undertaken.	Amber
Office Systems	Tolerant	Loss of day to day work tools	Intra day recovery times	Computacenter have run a full datacentre recovery test and restored systems to meet business needs.	Green
MDM	Neutral	Loss of key central system	Recovery within 2 working days	Successful test in 2018 met business needs	Green
Credence	Neutral	Loss of key central system	Recovery within 2 working days	Successful test in 2018 met business needs	Green
Swindon Stock systems	Neutral	Loss of warehouse stock control	Recovery within 2 working days	Systems are located in offisite data centres and the recovery capability has been tested and meets business needs.	Green

POL00423568

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Supply Chain	Averse	Unable to collect monies from branches Unable to deliver monies to branches Unable to replenish branch stock. Unable to fulfil Banking Framework	Alternate Depots, vehicles and cash processing capabilities within a working day.	Multiple depots across the UK can provide mutual support, as can alternative cash centres. Utilising third parties is also within current planning. Loss of Swindon is a single point of failure and plans for this are not tested.	Amber
NBSC	Averse	Unable to support branch operations	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Limited home working has also been tested.	Green
Communications	Averse	Unable to respond to any challenges	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
IT Management	Neutral	Unable to support contracts	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Finance Service Centre	Neutral	Unable to make payments or reconcile incoming monies	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Home working has also been tested. Manual work around for IT system failure in place.	Green
Treasury	Neutral	Unable to confirm funding requirements	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested. Home working has also been tested.	Green
POI Call Centre	Averse	Unable to manage incoming customer calls	Alternative recovery site	All systems are in DataCentres in France (Brexit challenge to be reviewed) and are resilient across two datacentres.	Green

POL00423568

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Mails Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Retail Management Team	Tolerant	Unable to support branch strategy	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Banking Framework Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Telco Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Bureau Management Team	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green

POL00423568

Business Functions	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Payzone	Averse	Unable to support outlets using Payzone technology	Alternative recovery office.	Contract in place with Sungard for the provision of office space to meet business needs. IT link to the Sungard solution in place. To be tested later in 2019	Amber
Finance	Tolerant	Unable to provide financial updates	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
POI	Tolerant	Unable to support contract	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
Bolton HRSC	Tolerant	Unable to respond to internal HR queries	Sungard solution in place	Proven ability to recover all operations at the alternative site has been tested.	Green
HR	Tolerant	Unable to support staffing needs	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green
LRG	Tolerant	Unable to provide internal operational support	If not operational for up to 4 days there would be minimal operational impact. Capability to work at an alternative location, be this home or another office.	Proven capability to work at home. Small Sungard solution in place for meetings to support home working.	Green

POL00423568

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
Royal Mail Group	Averse	Unable to collect from branches. Unable to deliver support to operations	Intra day recovery times	Greatest risk is strike for which Post Office and Royal Mail have worked together on identifying contingency solutions. Short term this would meet Post Office needs, within 3 days it would be difficult	Amber
VocaLink	Averse	Unable to provide ATM operations. Unable to provide faster payments.	2 hour recovery time	Three datacentres running continuously with load sharing. Zero down time tests run regularly. Observed testing and understanding has been shared with Post Office.	Green
FRES	Neutral	Unable to meet Bureau requirements	Recovery within 2 working days	Some small stock holding within Supply Chain would mitigate a short down time. Recovery capability is tested but on the same campus.	Amber
DWP	Averse	Unable to deliver POCA support	2 hour recovery time	Strategies in place and proven via testing annually	Green
Cardtronics	Neutral	Unable to meet ATM maintenance requirements	Recovery within 2 working days	ATM failures can be coped with for two days but after this repair and catch up of time lost would be essential.	Amber
Legal Advisors	Neutral	Unable to provide external legal advice	Recovery within 2 working days	Contractual recovery times and evidenced documentation meet Post Office needs.	Green

POL00423568

[*GROUP POLICY*]

[*Business Continuity Management*]

Version – V2.4

8.2

Chief Executive Endorsement

"Business continuity means we can continue to support Postmasters and serve customers when thing go wrong. It is therefore essential and we should support the policy at all times."

Alisdair Cameron, Chief Executive Officer, May 2019

POL00423568

contents

1 Overview 4
1.1 Introduction by the Policy Owner 4
1.2 Purpose 4
1.3 Core Principles 4
1.4 Business Continuity Objectives 5
1.5 Application 5
1.6 The Risk 5
1.7 Legislation 6
1.8 Industry Guidance 6
2 Risk Appetite and Minimum Control Standards 7
2.1 Risk Appetite 7
2.2 Policy Framework 8
2.3 Who must comply? 8
2.4 Minimum Control Standards 9
2.4.1 Threats 11
2.4.2 Approach 11
2.5 Implementation 12
2.5.1 Satisfying BCMS Requirements 12
3 Tools & Definitions 14
3.1 Tools 14
3.2 Definitions 14
4 Where to go for help 15
4.1 Additional Policies 15
4.2 How to raise a concern 15
4.3 Who to contact for more information 15
5 Governance 16
5.1 Governance Responsibilities 16
6 Control 17
6.1 Policy Version 17
6.2 Policy Approval 17

POL00423568

1.Overview

1.1. Introduction by the Policy Owner

The Business Continuity Manager has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter failures in normal operations. The Business Continuity Management Policy details the approach to implementing strategies and plans to minimise the impact to operations and restore operations in a time to meet business requirements. This approach ensures the risks to operations are known, the impact to operations of failure are understood and recovery priorities are based upon the tolerance to impact. The Policy is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2 Purpose

This Policy has been established to set the minimum operating standards relating to the management of the Business Continuity risks. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk and continuity of operations across the group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees and other stakeholders.

1.3 Core Principles

Post Office adopts the Business Continuity Institute's Good Practice Guidelines definition of business continuity as: "A holistic management process that identifies potential threats to an organisation, and the impacts to business operation those threats, if realised, might cause, and provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value- creating activities."

This Policy is consistent with "ISO22301", which is the Business Continuity International Standard. The purpose is to define the Group's policy with regard to business continuity management that is appropriate to its aims and objectives. This includes a framework for:

- Setting business continuity objectives;
- Satisfying appropriate legal, regulatory and contractual requirements;
- Continual improvement of the Business Continuity Management System ('BCMS'); and
- Key controls in respect of business continuity.

This policy should also be read in conjunction with other Post Office resilience, health & safety, and physical security related policies and procedures.

POL00423568

The following areas of Post Office's business are within the scope of the policy:

- All customer support centres including but not limited to, Finsbury Dials, Chesterfield and Bolton office
- All Supply Chain Locations
- All Directly Managed Branches
- All other Post Office Operational centres
- All external/outsourced Supply Chain Capability.

Out of Scope of this Policy:

- All IT systems – these are covered within the Information Disaster Recovery Policy

This policy's effective date will be determined by the date on which final approval is given by the appropriate governance forum

1.4 Business Continuity Objectives

Based on the requirements and factors set out in this document, the following major objectives are set for business continuity:

- Objective 1 - Comply with health and safety legislation at all times
- Objective 2 – Maintain stakeholder confidence
- Objective 3 – Maintain customer service levels
- Objective 4 – Minimise loss of revenue

The success of the BCMS will be judged on its ability to meet these overall objectives.

1.5 Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

The Policy should be considered within Change and Procurement and onboarding of new services, suppliers or business units.

The Policy applies to all business units and operations and should ensure plans, strategies and requirements are known for all areas to minimise the impact of any interruption.

The risk to the Group from Business Continuity is reviewed by the board annually.

1.6 The Risk

The Business Continuity Policy is designed to help mitigate the risk that normal operations are interrupted and not restored in a controlled and timely manner with the consequence that:

- Staff and Customers safety is at risk;
- Customers are unable to be served;
- Regulatory requirements are not met;
- Legal and contractual breaches occur;
- Income is affected; and
- Confidence in the Post Office's reputation is harmed.

POL00423568

1.7 Legislation

The Group is subject to a variety of legal and regulatory requirements which either apply directly or are imposed through contractual arrangements with key clients. These include, but are not limited to:

- Health and Safety legislation;
- Payment Card Industry – Data Security Standard compliance;
- Financial Services legislation;
- National and international standards e.g. ISO9001; ISO270001; and
- Consumer protection legislation.

1.8 Industry Guidance

ISO22301 is the accepted International Standard for Business Continuity. There are other Standards on Operational Risk, Information Security, Crisis Management and IT Disaster Recovery.

The Business Continuity Institute issues good practice guidelines The FCA

issues best practice guidelines

POL00423568

2 Risk Appetite and Minimum Control Standards

2.2 Risk Appetite

- The following risk appetite statements are relevant to Business Continuity:

Averse appetite for taking risks which might result in failure to maintain the service commitment in respect of customers in line with our social purpose and Government's policy on subsidy**.**

Neutral risk appetite for dissatisfaction related to BAU services recognising that in a complex business there will be a level of dissatisfaction as part of the normal course of business of achieving our commercial objectives.

Averse appetite for risk taking which would alienate or lose significant groups of profitable customers

Tolerant risk appetite for customer dissatisfaction caused by transformation, innovation and customer selection/profitability decisions.

Neutral appetite for risk taking which would have a detrimental impact on vulnerable customers. Post Office will take a balanced view, reflecting commercial implications of introducing safeguards and controls to protect vulnerable customers and the needs of those customers.

- Post Office takes its legal and regulatory responsibilities seriously and consequently has:

Tolerant risk appetite for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality

Averse risk appetite for not complying with law and regulations or deviation from business' conduct standards

Averse risk appetite for unethical behavior including staff Misfeasance, failure of, governance and control processes, critical financial reporting processes, and critical supply chain and business continuity processes.

- Post Office is committed to safeguarding the wellbeing of its people and therefore has:

Averse risk appetite associated to the health, safety and wellbeing of POL customers and colleagues in everything we do. This is paramount to every aspect of POL operation. This includes; loss of life, serious injury and non- compliance to regulation and policy

POL00423568

Post Office is committed to exploiting technological benefits to achieve market advantage. In recognition of this, Post Office has:

> ***Averse*** appetite for data loss/leakage that can lead to customer, commercial or reputational damage
>
> ***Neutral*** appetite for operational IT services
>
> ***Averse*** risk appetite for any serious impact to the confidentiality, integrity and availability of information, leading to financial loss, business disruption, public embarrassment or legal consequences.

Post Office recognises that it cannot completely eliminate business continuity risks. However, this policy sets out controls to reduce and/ or mitigate such risks.

This level of risk appetite will be applied to the risk assessments that are carried out as part of the BCMS and will determine the actions that need to be taken to mitigate risk to an acceptable degree.

2.3 Policy Framework

Post Office has established a suite of resilience and risk policies, on a risk sensitive approach which are subject to regular review. Other policies which may be relevant to business continuity include the following:

- IT Disaster Recovery
- Information Security
- Data protection
-

2.4 Who must comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of Risk and Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through willful disregard or negligence, this will be treated as a disciplinary offence.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

POL00423568

2.5 Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite:

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
All	BCMS is not fit for purpose. May lead to inadequate strategies and plans being implemented that do not meet business needs.	Annual review of the BCMS content and effectiveness. Internal Audit review	Updated on change of approach or discovery of gaps.	Business Continuity Manager Audit Manager	Annually
All	Risks the business and locations are exposed to are not known or are inadequately mitigated.	ISO22301 defines managing Business Continuity risks to include an assessment of : • Threats; • Vulnerabilities; • Impact & likelihood before risk treatment; • Risk treatment (e.g. reduction, removal, transfer); • Function responsible/ owner; and • Timescale and review frequency.	As risks are identified or occur and root cause analysis is completed risks and threats are added to the assessment matrix to ensure business areas continually challenge their strategies against new risks.	Business Continuity Manager. IT DR Manager. Facilities Manager. Location PICS. Business Leads.	Annually

POL00423568

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
All	The impact on operations of a business continuity incident is not clearly understood.	Impact is measured against agreed metrics and agreed times to ensure business areas can be compared and strategies implemented which are compatible with the risk and impact the operational area is exposed to.	Impacts are challenged and after any incident or exercise reviewed to ensure the assumed impact meets the actual impact observed.	Business Continuity Manager. Business Leads	Every two years or on change.
All	Recovery strategies do not meet business needs	Annual tests of strategies in place to ensure business has confidence and understanding in the capability	Strategies updated after tests or actual incidents to ensure they meet business needs.	Business Continuity Manager All business leads	Annually
All	Contingency plans are not in place or available.	Plans in place must be assessed by internal audit and annually the status presented to the RCC. Plans must be held by all managers and available in a single accessible repository.	Plans updated after tests or actual incidents to ensure they meet business needs.	All business leads Business Continuity Manager	Annually
BPT	BPT does not know the process to respond to a crisis	All BPT members are contacted and involved in crisis conference calls and undergo training.	BPT lists reviewed regularly and updated on change of roles or personnel.	Business Continuity Manager BPT members	Twice yearly
All	Staff are unaware of how to respond to a crisis	All staff are briefed and made aware of their responsibilities	Standard communications tools to brief staff, staff involved in testing, managers required to challenge their own plans and update them.	Business Continuity Manager All business leads	Ongoing
Building unavailable	Any key operational site may become unavailable for its purpose.	Risk assessments of sites are carried out annually by CBRE and POL. Strategies for the recovery of key operations per site are in place and annually tested.	Facilities and CBRE review risks regularly and provide options to enhance resilience levels to management.	Business Lead. Facilities Manager. Business Continuity Manager.	Annually. Upon moving in.

POL00423568

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
IT system failure	Any IT system can fail at any time.	This is managed under the IT DR policy and the IT COBIT process. All systems are documented and the impact of them failing documented. Resilient and DR capability is in place and managed by IT. This is tested annually.	Managed within the ITSCM role and covered in the Disaster Recovery Policy	CIO IT DR lead Business Leads Business Continuity Manager	Annually Upon Change. Upon impleme-ntation
Supply Chain distribution failures	Depots, Vans and operations may fail leading to routes and deliveries and collections not meeting business needs.	Plans and strategies to mitigate failures are in place and tested. Contingency planning for the loss of all forms of assets are tested.	Strategies updated after tests or actual incidents to ensure they meet Supply Chain needs.	Supply Chain lead Depot Leads Business Continuity Manager	Annually
Outsourced or supplier failure	Post Office relies heavily on suppliers and outsourcing to achieve its day to day operations. Any of these could fail or go out of business.	Part of the contract allocation and contract management covers business continuity. All suppliers commit to meet business continuity requirements and to test these. Contracts must contain appropriate BC and DR capability statements. Suppliers should demonstrate their recovery capability before a contract is signed, on review of the contract and if necessarily post any incident that affects them. Capability to restore operations in stated timeframes must be tested annually by all key suppliers. Suppliers to be categorised according to the risk their failure presents to Post Office. Many key suppliers will be within IT and the business consequence of an IT supplier failing must be shown to be mitigated by IT DR tests within these suppliers.	Contracts challenged if gaps are found, suppliers required to demonstrate their capability and contracts reviewed if gaps identified. Business areas required to implement plans to cover gaps in suppliers recovery capability.	Contract owner. Area dependent on contract. Business Continuity Manager. IT DR manager	Annually

POL00423568

Risk Area	Description of Risk	Preventative Controls	Corrective Controls	Who is responsible	When
Staff unavailable	Post Office staff are key to the success of day to day operations. At any time due to weather, health or any scenario staff may be unable to work.	Identification of single point of failure staff is undertaken within the contingency planning.	Key roles must be documented and where possible dual role training undertaken. As a working example the dependency on skilled drivers is key to supply chain and this is mitigated by the Rapid Response Team when required.	All business leads HR leads Business Continuity Manager	Ongoing

Post Office Limited - Risk and Compliance Committee-04/07/19

POL00423568

2.5.1 Threats

Post Office plans for the worst case scenario and does not work to specific threats unless they are beyond the scope of the risks planned for. Threats continue to vary and these will be used to define scenarios for exercises. Threats include:

- Weather related events
- Infrastructure failure
- Pandemic
- Cybercrime
- Environmental disasters
- Terrorism
- Industrial Action

2.5.2 Approach

In the approach to implementing, managing and reviewing business continuity capability the Post Office will:

- Create a Business Continuity Management System in line with ISO Standards showing the detailed approach to implementing and managing business continuity;
- Complete Risk and Impact assessments of tangible and intangible losses. To include an understanding of contractual and regulatory obligations, potential causes of risks, and impact of events both in terms of direct financial loss, cash flow interruption, customer impact, operational consequences, reputational impact and legal/regulatory impact. These assessments allow prioritisation of time and resource to implement recovery solutions;
- Develop and document strategies and plans to address key risks;
- Implement plans and recovery strategies (eg resilient IT, offsite recovery locations etc);
- Manage the central and local storage of plans;
- Annually (or more frequently) review plans;
- Consider impact of change activity on plans as part of major change activity;
- Create, manage and facilitate Post Office crisis response;
- Report all incidents and their impact;
- Test all strategies to ensure they meet business requirements;
- Integrate with IT recovery capability to ensure it meets business requirements;
- Train staff in the contingency plans and their roles and responsibilities;
- Complete root cause analysis when there is a (material) incident and review the control framework to include 'lessons learned';
- Embed appropriate and proportionate contractual requirements in contracts with suppliers and outsourcers including reporting, audit and rectification rights;
- Ensure there is regular oversight/testing of supplier and outsourcer obligations;
- Report twice yearly on progress against these approach steps.

POL00423568

2.6 Implementation

The approach to implement business continuity within Post Office are defined within this Policy. These are the fundamental steps required which are led by business areas, facilitated by the Business Continuity Manager and are not subject to frequent change. The Post Office GE will ensure that adequate funding is available for activities identified in the implementation and ongoing support of the business continuity process.

Amendments to the Business Continuity objectives will be managed through the standard Post Office change management process if required.

2.6.1 Satisfying BCMS Requirements

Senior Managers commit to the provision of the appropriate resources to establish and maintain the BCMS and its outputs.

Regular review of the BCMS. This is conducted by the Business Continuity Manager on an annual basis, ensuring that objectives are being met. Evaluation of the current capability is undertaken and any issues identified through this audit programme and management processes are reported to the RCC. Management review includes departmental and other management meetings and document review.

Role definition and responsibilities are defined in the BCMS and reviewed by the Business Continuity Manager to ensure that colleagues understand the roles they are required to fulfil, and that they have the appropriate skills and competences to do so. These controls are necessary to ensure the continued BCMP success and to mitigate risk. Training will be provided where gaps in competency are identified and regular reviews of staff capability will be undertaken within departmental exercises.

Use of third parties. Post Office uses third parties, both internal and external, in the delivery of products and services. The ability to continue to provide these services or restore them should a supplier fail is key to Post Office operations and part of all contracts. This supplier capability will be evidenced by documentation and records, including contracts, meeting minutes and IT DR and BC test reports.

Continual improvement:

To ensure the approach to implementing and managing the BCMS is enhanced in an ongoing manner Post Office will:

- Consider effectiveness of the BCMS across all business areas and end to end systems, processes within scope;
- Enhance current processes to bring them in to line with best practice (as defined within ISO 22301);
- Increase the level of proactive continuity planning across Post Office;

POL00423568

- Achieve an enhanced understanding of and relationship with the business units to which the BCMS applies;
- Review relevant metrics (impacts, risk etc) on an annual basis to assess their appropriateness, or to make changes to them based on collected historical data and feedback or in response to incidents;
- Obtain ideas for improvement via regular review meetings with stakeholders.

Ideas for improvement may be obtained from any source, including but not restricted to: Customers; Suppliers; Colleagues; Risk Assessments & Audits.

In order to evaluate any proposed improvements to the BCMP, the following criteria would be applied:

- Cost;
- Business benefit;
- Risk;
- Implementation timescale; and
- Resource requirement.

Accepted improvement proposals will be prioritised, and planned according to standard project management principals.

POL00423568

3 Tools & Definitions

3.2 Tools

None in place

3.3 Definitions

Term or Acronym	Description
BCMS	Business Continuity Management System, the set of controls in line with ISO22301 to implement and manage business continuity
BC	Business Continuity
ITDR	IT Disaster Recovery, the recovery of IT systems and data
ISO 22301	The International Standard for Societal Security (Business Continuity).

POL00423568

4 Where to go for help

4.2 Additional Policies

This Policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/postoffice/Pages/policies.aspx

4.3 How to raise a concern

Any Post Office employee who has concerns about a failure to comply with this policy has a duty to:

- discuss the matter fully with their Line Manager; or,
- discuss it directly with their Head of Business Unit; or,
- Report their suspicions by telephoning Grapevine on GRO
- If either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect [activity in breach of policy] to write, in confidence, to the Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ.

4.4 Who to contact for more information

If you need further information about this policy or wish to report an issue in relation to this policy, please contact Tim Armit – Business Continuity Manager by email at **tim.armit** GRO

8.2

POL00423568

5 Governance

5.1 Governance Responsibilities

Post Office's Board of Directors have overall responsibility for ensuring that Post Office has a framework to ensure compliance with legal, regulatory and contractual requirements. The Board is kept abreast of relevant matters relating to the management of business continuity by reports from its committees including its ARC Committee. The key individuals and their specific responsibilities in relation to this policy are:

- The General Counsel is a member of the Post Office Executive team and is the Group Executive Owner and Policy Sponsor, accountable to the Board.
- The Group Business Continuity Manager is the Policy Owner who is responsible for:
    - Day to day implementation of and compliance with this policy and is accountable in this regard to the General Counsel;
    - Ensuring that there is an annual review of this Policy and tests compliance across the Group.
    - Providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

Post Office's internal systems of business continuity risk control ensure that controls are regularly independently assessed for effectiveness, suitability and adequacy. In addition, Internal Audit will periodically test compliance with this policy.

POL00423568

6 Control

6.1 Policy Version

Date	Version	Updated by	Change Details
19th May 2016	1.0	Jon Waples	First signed version
25th Feb 2018	2.0	Tim Armit	For review and signature
8th March 2018	2.2	Tim Armit	Typo changes

6.2 Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL R&CC	13th March 2018
POMS R&CC	27th March 2018
POL ARC	
POMS ARC	

Policy Sponsor: **Group Director of Legal, Compliance & Governance**

Policy Owner: Business Continuity Manager

Policy Author: Business Continuity Manager

Next review: *date of next review 01 02 2019*

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

POL00423568

ABC Annual Review 2018-19

Author: Sally Smith | Sponsor: Ben Foat | Meeting Date: 4th July 2019

Executive Summary

Context

As part of our Anti-Bribery and Anti-Corruption (ABC) obligations, this report provides an overview of Gifts & Hospitality reporting for the financial year 2018/19 and provides a summary of changes as part of the annual policy review.

Questions addressed in this paper

- What issues have been highlighted based upon the review?
- What actions need to be undertaken to address any issues?
- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The reporting and approval of gifts and hospitality have continued to improve, albeit some common errors do recur and it is likely that there is still under-reporting. Quarterly checks of adherence to the minimum control standards set out in the ABC policy have not highlighted any material issues.
2. Further communications and awareness are planned for 2019/20, and the annual ABC training is being enhanced
3. A new appendix has been added to the ABC policy to summarise the policy relating to Gifts and Hospitality to help improve reporting and approval
4. There are no significant changes that impact the business

Input Sought

The committee is asked to review the contents of this report, approve the updated ABC Policy and Corporate website statement and consider whether any further actions should be taken to improve gifts and hospitality reporting.

POL00423568

The Report

Summary of ABC activities 2018-19

5. The House of Lords set up an ad hoc Select Committee in 2018 to conduct a post-legislative review of the Bribery Act 2010. They published their findings in March 2019 confirming that the Bribery Act 2010 is "an exemplary piece of legislation" which sets the global benchmark for anti-bribery and corruption legislation.
6. No change to the existing law is anticipated, although some recommendations relating to law enforcement investigations, MOJ guidance and penalties/deferred prosecution agreements were made
7. The importance of a risk assessment was emphasised, stating that all businesses, must conduct a properly documented risk assessment to ensure they make an informed decision about the level of risk their business faces to determine whether they require any safeguards.
8. Externally, there have been a number of high profile bribery and corruption cases both in the media and presented to the Joint Money Laundering Intelligence Taskforce, highlighting law enforcement and regulatory focus on this area.
9. Annual training was delivered to all employees in September 2018 and on-going completion is tracked on a monthly basis to ensure that new joiners are completing.
10. Quarterly reporting is provided to all GE members summarising overall Post Office Gifts & Hospitality reporting and highlighting any breaches or concerns for each GE
11. There have been 4 communications issued relating specifically to Gifts and Hospitality reporting.
12. The Gifts & Hospitality tool homepage has been updated with detailed user guides for each stage of reporting and approval and the Selenity Expenses portal has been updated to require claimants to capture the Gifts & Hospitality approval reference when they are making expense claims for gifts or hospitality offered.
13. Work is being undertaken with the People and Culture Director in relation to raising awareness of ethical behaviour in business and promoting the importance of compliance with Post Office's ABC policy.
14. The Corporate website ABC statement has been reviewed as per Appendix A.

Summary of Gifts & Hospitality received and offered 2018-19

15. Analysis of the 2018-19 Gifts & Hospitality Register has highlighted that the quantity and quality of submissions compared to 2017/18 has continued to improve (please see Appendix B & C for data), although it is still believed that some gifts and hospitality are not being reported by recipients/offerors:
    - In 2017/18 there were 27 gift reports totalling £1,521 and 195 hospitality reports totalling £33,673.07
    - In 2018/19 there were 47 gift reports totalling £4,918.64 and 188 hospitality reports totalling £38,703.54
16. An occasional delay between the user uploading a request and it appearing on their submission page has led to some individuals re-submitting resulting in duplicated reports. A warning message has been included on the tool advising employees to contact the Gifts and Hospitality mailbox and the issue has been communicated to the business though One Comms and escalated to IT to resolve.
17. In the reporting period, the following common breaches were identified:
    - As reported last year, we are still identifying instances of employees accepting gifts of cash or cash equivalent (e.g. gift cards). Further Intranet articles were published January 2019 reminding staff about not accepting cash.
    - Whilst there has been a decrease in users submitting retrospective requests, instances remain where individuals are reporting hospitality either on the day of, or following the event they are attending. A number of communications have

POL00423568

been cascaded to the business reminding employees they must not attend or accept hospitality until the offer has been reported and accepted by their Line Manager.

- Colleagues continue to provide insufficient information within the title description. Additional examples have been added alongside the title description field to help reduce these errors. Submitters have also been contacted in order to provide more detailed descriptions where required.

18. A review of the external companies that have offered hospitality to Post Office in 2018/19has not identified any significant issues, and the top 8 are detailed below:

External Party Name	Volume	Volume of People	Total Value
Womble Bond Dickinson	5	24	£4,870.00
FRES*	18	15	£3,729.60
Trethowans LLP	3	30	£3,000.00
ISF	2	2	£2,510.00
Fujitsu Telecoms	4	12	£2,190.00
AT Kearney	3	5	£1,800.00
DUCK CREEK	1	1	£1,500.00
Fujitsu	9	19	£1,095.00

*Note in 2017/18 FRES were the largest donor with 22 offers totalling £2,580

Planned actions to address issues:

19. The following activities are planned to improve the quality and effectiveness of gifts and hospitality reporting and approval:

- 2019/20 ABC Communications Plan has scheduled Gifts & Hospitality reminders to Back Office and DMBs in April, July and November to target the busiest periods for offering and receiving gifts and hospitality.
- The ABC annual compliance training for 2019/20 will be delivered in September – the content is being enhanced and improved
- The Gifts & Hospitality policy appendix (see para 22 below) will be posted on the reporting tool homepage to assist reporters and approvers
- The Financial Crime team are working with Executive Assistants, as they are frequent users, to review functionality and identify possible improvements that could reduce common breaches and errors.

Why do we need to review this Policy?

20. The Policy was last reviewed and approved by the R&CC in July 2018.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

21. There have been no legislation changes in the past year although

22. Minor amends have been made:

- An appendix has been created to summarise and clarify the Gifts & Hospitality policy requirements and help reduce reporting and approval errors.
- Following queries received through the year and review of industry best practice and to ensure transparency, an enhanced control has been introduced in respect of donations and sponsorship.

How did we develop these recommendations?

POL00423568

23. A review of bribery and corruption cases and penalties publicly reported over the last 12 months and cases that the Financial Crime team has been involved in via the Joint Money Laundering Intelligence Taskforce, together with policy queries and issues that have arisen over the previous 12 months.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

24. No material changes are required to comply with this updated Policy.
25. The Financial Crime Team are developing a central donations and sponsorship process and register and incorporating into the ABC training to be delivered in September.
26. The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their review of the Gifts and Hospitality Tool and any other reported issues. Any control gaps identified will be reported to the RCC as required (see Appendix D for latest assurance status).
27. The Financial Crime Team provide quarterly reports to Group Executive members.
28. Every six months, as part of the Group Executive declaration the members are required to confirm that the Policy has been correctly applied in their business area.

What will the impact be on our wider business?

29. Increased transparency of the ABC framework and commitment to maintaining visible compliance with the applicable legislation.
30. Reinforcement that the failure to comply with the requirements of ABC Policy by any employee will be regarded as a significant breach impacting on the Post Office's risk and control management environment and may lead to disciplinary action up to and including dismissal and possible prosecution.

What would the impact be of delaying approval?

31. Risk that the group breaches the Bribery Act 2010 by not having up to date policies and procedures to prevent bribery by any person or company who operates on our behalf.
32. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.
33. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Sally Smith
MLRO & Head of Financial Crime
27th June 2019

POL00423568

GROUP POLICIES

Anti-Bribery and Corruption Policy

9.1

Version – V3.1

Chief Executive's Endorsement
The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure the highest standards of financial crime prevention, detection and management are maintained.

POL00423568

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 4
1.5. Types of Bribery and Corruption Risk 4
1.6. Legislation 5
1.7. FCA Rules 6
2. Risk Appetite and Minimum Control Standards 7
2.1. Risk Appetite 7
2.2. Policy Framework 7
2.3. Who Must Comply? 8
2.4. Gifts and Hospitality Tool 8
2.5. Minimum Control Standards 9
3. Definitions ..... 17~~16~~
3.1. Definitions ..... 17~~16~~
4. Where to go for help ..... 18~~17~~
4.1. Additional Policies ..... 18~~17~~
4.2. How to raise a concern ..... 18~~17~~
4.3. Who to contact for more information ..... 18~~17~~
5. Governance ..... 19~~18~~
5.1. Governance Responsibilities ..... 19~~18~~
6. Control ..... 20~~19~~
6.1. Policy Version ..... 20~~19~~
6.2. Policy Approval ..... 20~~19~~
Company Details ..... 20~~19~~

9.1

POL00423568

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the design and implementation of controls to prevent or deter Bribery and Corruption. Anti-Bribery and Corruption is an agenda items for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of our Bribery and Corruption risks throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, employees[2] and other stakeholders.

1.3. Core Principles

To offer a bribe is a criminal offence; bribery is an offer, promise, payment, request, or agreement to receive anything of value from any person or entity in order to induce that person to perform their roles improperly.

In order to prevent Bribery and Corruption the governance arrangements described in this Policy are based upon the following core principles:

- The Group is committed to and oversees the implementation of a Policy of zero tolerance, recognising that bribery is contrary to fundamental values of integrity, transparency and accountability and undermines the Group's effectiveness;
- Post Office has devised a robust Policy and associated procedures (set out in this document) which are proportionate to the risks and complexity of the Group;
- A bribery risk assessment is an integral part of our Group's overall and ongoing risk management process;
- Post Office must assess the risk associated with entering into joint ventures, partnerships or contracting arrangements with other entities and must carry out periodic due diligence based on that risk assessment. This includes ensuring that these organisations have policies and procedures which are equivalent to the Group's own procedures;
- The Group undertakes a training and awareness program to ensure employees are aware of the potential risks, how bribery might affect them, what they should do if they are offered a bribe, and the consequences should they be found to have made or received a bribe;
- The interests of Policyholders and other stakeholders are protected by ensuring that excessive powers are not delegated to individuals;

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and Post Office Management Services Limited.
[2] In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.

POL00423568

- Decisions taken by management are consistent with the Group's strategic objectives and risk appetite, which are approved by the Board;
- Appropriate conduct is demonstrated in executing the requirements contained within the Policy;
- Every member of staff is responsible for understanding and managing the risk they take on behalf of the Group and for ensuring that they act within accordance to them;
- All employees are required to comply with Group Policies.

1.4. Application

This Policy is applicable to all areas within the Group and defines the minimum standards to control financial loss, customer impact, regulatory breaches and reputational damage in line with the Group's Risk Appetite.

In exceptional circumstances, where risk sits outside of the Group's accepted Risk Appetite a Risk Exception can be granted. Further information in relation to the risk exception process, together with a template can be found here.

While Post Office does not tolerate events that are criminal in nature and which may give rise to unacceptable and illegal behaviour, it recognises that despite its many endeavours, it is not possible to eliminate all risks of internal and external Bribery and Corruption. As a result Post Office may incur losses, and therefore takes a risk based approach to Bribery and Corruption.

For definitions please see section 3.1.

The risk to the Group in relation to Bribery and Corruption is reviewed by the board on a regular basis.

9.1

1.5. Types of Bribery and Corruption Risk

Post Office is exposed to a number of the above risks relating to Bribery or Corruption. These risks include, but are not limited to, the following:

1. **Payment Risks** –for example, facilitation payments, gifts & hospitality, client training programmes, charitable or political donations, ex-gratia payments/ legal settlements. This would also include the offer of sponsorships or grants.
2. **Third Party/Associated Party Risks** –third parties who provide services on behalf of the Post Office Group engaging in bribery or corruption while performing such services. The scope of this could include agency operators within the Post Office network and suppliers procured through the business or through the Procurement Team. Examples of Associated Parties include agents, consultants, suppliers, introducers, and intermediaries.

POL00423568

3. **Employment Risks** –Post Office employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities at the Post Office or offering or providing work opportunities, paid or unpaid, to Connected Individuals[3], or otherwise using employee connections to improperly obtain business or secure an advantage for Post Office. Employment opportunities (including work experience, secondments, etc.) have a value to the recipient and/or their close family members and may be considered to be bribes if used to improperly obtain or retain business or secure an advantage for Post Office.

4. **Inducement Risks -** Post Office must take reasonable steps to ensure that it, and any person acting on its behalf, does not:
   - Offer, give, solicit or accept an inducement; or
   - Direct or refer any actual or potential business in relation to another person on its own initiative or on the instructions of an associate; if it is likely to conflict to a material extent with any duty that Post Office Management Services owes to its customers in connection with an insurance mediation activity or any duty which such a recipient firm owes to its customers in connection with an insurance mediation activity.

5. **Gifts & Hospitality** –The offer of Gifts & Hospitality by or to third parties represents a clear risk of inducement or facilitation and Post Office therefore has clearly defined minimum control standards and ~~Group has a process~~ procedures for reporting and approving Gifts & Hospitality (both received and offered). Appendix A sets out the specific policy requirements and details of the process to be followed ~~of this~~ can be found on the Gifts & Hospitality reporting homepage here.

Commented [SS1]: Updated to reinforce requirements laid out in minimum control standards and reduce reporting and approval errors

1.6. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to):

- The Bribery Act 2010
- The Criminal Finances Act 2017
- Financial Conduct Authority (FCA) Rules and Guidance (to the extent that these apply – see 1.8 below)

Under the Bribery Act, it is an offence to:

- Directly, or indirectly offer, promise or give a financial or other advantage with the intention of inducing any person to perform a business activity improperly or to reward any person for doing so;
- Request, agree to receive or accept a bribe, i.e. to receive a financial or other advantage with the intention of performing a business activity improperly;
- Bribe a foreign public official;
- Fail to prevent bribery by any person who perform services for or on behalf of a company ("corporate offence").

Post Office is subject to the Bribery Act 2010 (Bribery Act) and could become criminally liable as a result of an act of bribery or corruption by its employees or a third party operating on our behalf.

The Bribery Act has extra-territorial effect which means that the actions of Post Office or a third party operating on our behalf outside of the UK may fall within the scope of the

[3] Connected Individuals means those individuals who are known to have close connections to existing or prospective clients or suppliers, Public Officials, Politically Exposed Persons (PEP) or using employees' connections to improperly obtain business or secure an advantage for Post Office.

POL00423568

Act. In the context of Post Office, this could apply in scenarios such as where a Post Office contractor or supplier resides outside the UK.

Post Office can be held liable unless it can demonstrate that it has in place "adequate procedures" designed to prevent this type of misconduct. The controls outlined in this Policy, including appendices, assist Post Office in preventing and detecting corrupt conduct and form an essential component of Post Office's adequate procedures.

1.7. FCA Rules

Post Office Limited is an Appointed Representative of the Bank of Ireland and Post Office Management Services Limited (POMS) and is contractually required to comply with certain regulatory requirements. As such the Group as a whole is obliged to ensure there are adequate systems and controls are in place to mitigate Financial Crime risks.

POMS is a directly regulated firm with the FCA is directly exposed to regulatory fines and censure if the FCA determine that the systems and controls associated with this Policy are not effectively implemented.

This Policy contributes to Post Office's compliance with these regulatory and contractual obligations.

POL00423568

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[4]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented a product or transaction may still sit outside the agreed Risk Appetite. In this situation, a risk exception waiver will be required[5].

2.2. Policy Framework

Post Office has established a suite of financial crime policies and procedures, on a risk sensitive approach which are subject to an annual review. The Policy suite is designed to combat money laundering, terrorist financing, bribery and corruption and adhere to relevant Sanctions regimes. These have been developed to comply with applicable legislation and regulation and covers the following specifically:

- The identification of potential financial crime risks
- On a risk sensitive approach, performing due diligence at on-boarding, periodic basis and payment on third parties who perform services for or on behalf of us.
- Maintaining appropriate records for at least the minimum UK prescribed periods.
- Completing compliance oversight monitoring to test the Group's controls and confirming effectiveness and adherence to financial crime policies.
- Establishing and maintaining Standards for Management Information on Financial Crime. This includes, but is not limited to, record keeping, reporting of suspicious activity and details of staff training.

The Anti-Bribery and Corruption Policy is a key Policy under the Financial Crime Policy framework and should be considered and read in conjunction with the overarching Financial Crime Policy where relevant.

[4] The Risk appetite was agreed by the Groups Board January 2015
[5] For more information in relation to Risk Exception waivers please see section 1.4

POL00423568

2.3. Who Must Comply?

Compliance with this Policy is mandatory for all Post Office employees and applies wherever in the world the Group's business is undertaken. All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this Policy with their own equivalent Policy.

Where non-compliance is identified the matter must be referred to the Director of Compliance and the Group Legal Director. Any investigations will be carried out in accordance with the Investigations Policy. Where is it identified that that an instance of non-compliance is caused through wilful disregard or negligence, this will be treated as a disciplinary offence.

All Post Office employees are required to report any knowledge or suspicions in relation to Bribery or Corruption to Grapevine. As such all business units are required to have a process in place for reporting Bribery or Corruption incidents to Grapevine by telephone on GRO For more information in relation to reporting knowledge or suspicions please see section 3.2.

The next page sets out the minimum control standards that the Group has implemented to control these risks.

2.4. Gifts and Hospitality Tool

The purpose of the Gifts and Hospitality Tool is to make it easy for our employees to accurately record the offering and acceptance of gifts and hospitality throughout the Group. For more information in relation to the tool and how to use this, please see the below links:

Commented [SS2]: Update links

9.1

The Gifts and Hospitality Tool can be found here.

Instructions on how to complete the tool can be found here.

The procedure for completing the Gifts and Hospitality Tool can be found here.

POL00423568

2.5. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Appointment and Activities of Consultants and Contractors	Failure to ensure that Consultants and Contractors comply with the Group's anti-bribery and corruption policy may lead to criminal prosecution and damage to the Post Office brand or reputation.	Preventative Control: Our contracts require Consultants and Contractors to comply with the Group's anti-bribery and corruption policy. A clause is included within Consultants and Contractors contracts requiring them to comply with the Group's anti-bribery and corruption policy.	Procurement	Ongoing where required
Charity Donations and Sponsorship	Insufficient controls may lead to the donation of money to an unregistered charity, or the acceptance of a donation by Post Office which could be interpreted as bribery and result in reputational damage.	Preventative Control: Where the Group, a team or an individual has selected a particular charity to support, they are required to validate that charity against the Charity Commissions website. More information can be found here. Where a supplier or third party requests that Post Office makes a charitable donation, or offers to make a donation to Post	All employees All employees	Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		Office, Post Office ensures that the donation is not linked to any business or services provided to or by that supplier or third party. Any ~~cash~~ donations or sponsorship (cash or otherwise) should be approved by the relevant GE member to ensure appropriateness and the details recorded on the central donations register Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. Outsource providers, clients & suppliers must maintain records to evidence that staff have received adequate and regular training. Detective Controls: Pass rate and number of test attempts is monitored to identify risk areas and any additional training or guidance required.	GE are responsible for approval of ~~cash~~ donations and sponsorship The Financial Crime team maintain the donations register Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training Financial Crime Team is responsible for reviewing training effectiveness	Ongoing

Commented [SS3]: Control amended to ensure there is a central record of all donations and sponsorship.

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Conflicts of Interest	The acceptance of hospitality or gifts from third parties could lead to bias or undue influence, or the perception of such, in how individuals exercise their duties and responsibilities.	Preventative Control: The Group operates a procedure to ensure Gifts and Hospitality may not be offered or accepted where they could bias or influence how individuals exercise their duties and responsibilities. All employees are made aware of and are expected to comply with the gifts and hospitality procedures.	All employees	Ongoing
Employment Risks	Failure to identify employees requesting or receiving something of value from a third party in exchange for providing employment or work opportunities may result in the loss of Group stakeholder support.	Preventative Control: Any form of employment or work opportunities (paid or unpaid) must be reviewed and approved in accordance with HR policies and procedures prior to employment.	All employees	Ongoing
Gifts	Inadequate controls may lead to employees accepting gifts that are not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly all gifts of £20 and over which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined.	Each employee is responsible for ensuring that all gifts offered or received are recorded.	Ongoing Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		No employee may accept cash (or cash equivalent) gifts. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. Corrective Control: Where discrepancies of non-conformance with gifts and hospitality reporting are identified, line management should consider action under the Conduct Code	Line managers are responsible for ensuring the gift complies with policy and is reasonable and for approving or declining the acceptance of a gift Group Executive are responsible for approving or declining any offers over £100 Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register. Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing Ongoing
Hospitality	Inadequate controls may lead to employees accepting hospitality that is not appropriate, proportionate or within policy resulting in reputational damage or criminal prosecution.	Preventative Control: All employees must report correctly any hospitality which they receive or offer using the Gifts & Hospitality tool, whether accepted or declined. Before accepting or giving hospitality an employee must receive written approval from their line manager.	Each employee is responsible for ensuring that all hospitality offered/received are recorded Line managers are responsible for ensuring the gift complies with policy and is reasonable	Ongoing Ongoing

Commented [SS4]: Control added in line with HR policies

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The hospitality must be reasonable (not lavish or extravagant), proportionate to its purpose and must ordinarily be below £200 per person in value. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually. Corrective Control: Where discrepancies of non-conformance with gifts and hospitality reporting are identified, line management should consider action under the Conduct Code	and for approving or declining the acceptance of hospitality Group Executive are responsible for the approving or declining of any offers of hospitality over £200 Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing Ongoing
Payment Risks	Offering facilitation payments, gifts & entertainment, client training programmes, charitable or political donations, ex-gratia payments or legal settlements that are not	Preventative Control: All employees are required to comply with the conflicts of interest policy which can be found here. All employees are required to comply with the Gifts and	Each employee is responsible for ensuring that all hospitality and gifts offered or received are recorded	Ongoing Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	justifiable or proportionate may result in reputational damage or criminal prosecution.	Hospitality procedure which can be found here. The acceptance of discounted or complimentary training courses which would usually incur a cost are classified as Gifts and Hospitality and employees are required to report these using the Gifts & Hospitality Tool. The payment of ex-gratia payments or legal settlements are strictly controlled and must be submitted to the Group Legal Director for approval. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	Line managers are responsible for approving or declining the acceptance of a gift or hospitality. Group Executive are responsible for the approving or declining of any offers of gifts or hospitality over the agreed amounts Financial Crime Team is responsible for reviewing and monitoring the Gifts and Hospitality register Group Legal Director is responsible for reviewing and signing off as required any ex-gratia payments or legal settlements as requested from the Business. Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	Ongoing Ongoing Ongoing
Political Donations/Lobbying	Employees making or soliciting political donations on behalf of Post Office may	Preventative Control: Before giving or offering Hospitality to or from a political	Each employee is responsible for ensuring that all Gifts & Hospitality	Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
	result in criminal prosecution.	party, approval must be obtained from a GE Member. The giving of political donations or gifts on behalf of the group to a Politician or a Political Party is strictly prohibited. Post Office has a Group wide training programme to ensure that all customer facing staff, back office staff and contractors receive adequate training. Staff and contractors are required to complete training within 30 days of joining Post Office and annually.	offered or received is recorded Group Executive are responsible for the approving or declining of any offers of hospitality by a political party Financial Crime Team is responsible for reviewing the Gifts and Hospitality register Human Resources is responsible for any incidents where further action is required and ensuring completion of mandatory training	 Ongoing Ongoing
Procurement/Third Party Risk	Inadequate monitoring may lead to third parties engaging in bribery or corruption while performing services on behalf of the Post Office Group. This could result in criminal prosecution, loss of key contracts or reputational damage.	Preventative Control: Post Office ensures that any fees paid are proportional to the services being rendered or consistent with the market. New and existing contracts are reviewed on an ongoing basis to ensure that there is no risk of conflicts of interest. This includes ensuring that all parties	Chief Financial Officer Procurement	Ongoing Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		involved are aware of Procurement Lockdowns.		

The Group completes Annual Risk Assessments reviewing its bribery and corruption exposure and its compliance with the above key risk areas.

POL00423568

3. Definitions

3.1. Definitions

Bribery
Bribery is defined as the offer, promise, payment, request, agreement to receive anything of value whether directly or indirectly to or from any person or entity in order to induce that person or entity to perform their roles improperly or, in the case of a Public Official, in order to influence them with the intention of obtaining or retaining business or an advantage in the conduct of business.

Examples include an offer or promise to give anything of value to anyone to obtain or retain business for or on behalf of the Post Office or to obtain or fulfil a legal or regulatory requirement in furtherance of the Group's business. A bribe can take the form of a "reward" and be paid after the improper performance of the relevant duty or obligation.

Corruption
Corruption is defined as the misuse of entrusted power or public office for private gain.

Educational courses/conferences
Events that are offered by third parties without charge do not amount to hospitality. However, free places to attend courses or conferences that would otherwise attract a charge are covered by this procedure.

Facilitation Payment
A Facilitation Payment is a type of bribe and should be seen as such. A common example is where a government official is given money or goods to perform (or speed up the performance of) an existing duty. Within the UK these are strictly prohibited.

Gifts
Gifts refers to a physical gift and includes the offer to a specific individual or team with the exception of low value promotional items costing under £20 each, such as pens, calendars, diaries, notepads and paperweights.

Hospitality
Invitations to attend events which have a social element (whether or not they are at the same time as or linked to a business meeting) and where the cost of a 'ticket' (participation) is free of charge or reduced in price when otherwise there would be cost attached to it. This would include things such as tickets to a sporting event, tickets to a concert or a corporate dinner.

Inducement
An inducement is a benefit offered to a firm or any person acting on its behalf, with a view to that firm, or that person, adopting a particular course of action. This can include, but is not limited to, cash, cash equivalents, commission, goods, hospitality or training programmes.

Third Party funded trips
Travel/accommodation that is funded by third parties is covered by this procedure as a form of 'hospitality'.

POL00423568

4. Where to go for help

4.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach in this Policy should report this without any undue delay.

In case of bribery or corruption concerns or whistleblowing, staff may contact:

- their line manager,
- a senior member of the HR Team, or
- if either or both are not available, staff can contact the Post Office's General Counsel, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO
- or via a secure on-line web portal: http://www.intouchfeedback.com/postoffice

Post Office encourages members of the public or people not employed by us who suspect bribery or corruption to write, in confidence, to the **Chief Executive's Office, Finsbury Dials, 20 Finsbury St, London EC2 9AQ.**

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

9.1

POL00423568

5. Governance

5.1. Governance Responsibilities

The Policy sponsor, responsible for overseeing this Policy is the General Counsel of Post Office Limited.

The Policy owner is the Director of Compliance who is responsible for ensuring that the Financial Crime Team conducts an annual review of this Policy and tests compliance across the Group. Additionally the Director of Compliance and the Financial Crime Team are responsible for providing appropriate and timely reporting to the Risk and Compliance Committee and the Audit and Risk Committee.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

POL00423568

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
Date	Version	Updated by	Change Details
November 2016	1	Georgina Blair	Roll out of Final version
June 2017	1.2	Thomas Richmond	Updated in line with comments from stakeholders
July 2017	1.3	Sally Smith	POL R&CC approval
September 2017	2	Sally Smith	Final Version approved by ARC
June 2018	2.1	Sally Smith	Annual revisions
July 2018	2.2	Sally Smith	POL R&CC approval
July 2018	2.3	Sally Smith	POL ARC approval
September 2018	2.4	Sally Smith	POMS ARC approval
September 2018	3	Thomas Richmond	Final Version approved by ARC's
July 2019	3.1	Sally Smith	Annual review

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date Approved
POL R&CC	10th July 2018
POL ARC	31st July 2018
POMS ARC	20th September 2018

Policy Sponsor: Group Director of Legal, Risk & Governance

Policy Owner: Director of Compliance

Policy Author: Head of Financial Crime

Next review: July 2019

9.1

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081

POL00423568

Appendix A

GIFTS AND HOSPITALITY POLICY

All gifts and hospitality received and offered by Post Office employees must be reported on the central register and **pre-approved prior to acceptance***. This to ensure that Post Office is transparent in its dealings with third parties and suppliers and to enable senior management and the GE to monitor the level of gifts and hospitality both received and offered across the business.

All employees receive annual training as part of the Anti-Bribery & Corruption module within 30 days of joining Post Office and annually.

Gifts:

- All employees are responsible for ensuring that full details of gifts are accurately recorded including the recipients details and a description of the gift, dates of offer and the amount – if a gift is received by a Post Office employee, then an approximate value can be recorded, if known, or the offeror must be contacted and asked the amount so that this can be properly recorded.
- All gifts of £20 and over which are received or offered must be recorded using the Gifts & Hospitality tool, whether accepted or declined by the receiver.
- Line managers must review and approve all gifts over £20. If a gift is over £100, then this must also be reviewed and approved by the GE member for that area
- Before any gift is offered by a Post Office employee, they must refer to the relevant cost centre budget holder for approval before proceeding
- No employee may accept cash (or cash equivalent) gifts (including gift cards).
- The value of the gift must be appropriate and proportionate for the roles and relationship with the client
- Any offer must have a clear and demonstrable link with a legitimate business purpose, gifts must never be accepted from a third party who is tendering for business with Post Office.
- Recipients or offerors must consider if an offer could be viewed by an external party as inappropriate. Guidance can be sought from line management or by raising a query via gifts.hospitality GRO

Hospitality:

- All employees are responsible for ensuring that full details of hospitality are recorded including the recipients details and a description of the hospitality, details of venue/event, dates of offer and event and the amount – if the amount is not known the offeror must be contacted and asked the amount so that this can be properly recorded
- All hospitality which is received or offered must be recorded using the Gifts & Hospitality tool, whether accepted or declined by the receiver.
- Line managers must review and approve all hospitality. If hospitality is over £100, then this must also be reviewed and approved by the GE member for that area
- Before any hospitality is offered by a Post Office employee, they must refer to the relevant cost centre budget holder for approval before proceeding
- The value of the hospitality must be appropriate and proportionate for the roles and relationship with the client
- Any offer must have a clear and demonstrable link with a legitimate business purpose, hospitality must never be accepted from a third party who is tendering for business with Post Office.
- Recipients or offerors must consider if an offer could be viewed by an external party as inappropriate. Guidance can be sought from line management or by raising a query via gifts.hospitality GRO

POL00423568

- Small offers of hospitality such as tea, coffee, sandwiches, etc. do not need to be recorded via the gifts and hospitality tool, but the recipients details must be recorded fully on the expenses claim via Selenity Expense reporting tool

* Where it is not possible to record gifts and hospitality received prior to receipt, for example where a gift is received unexpectedly, or where a client offers to pay for lunch, then this must be recorded **on the next available day** and the reasons for late approval should be added in the comments box. For offers of hospitality verbal approval from a more senior manager should be obtained.

POL00423568

Whistleblowing Review 2018-19

Author: Sally Smith | Sponsor: Ben Foat | Meeting Date: 4th July 2019

Executive Summary

Context

This report provides an overview of the financial year 2018/19 as part of our obligations to protect whistleblowers and support individuals who raise genuine concerns under the Whistleblowing Policy. The report also provides a summary of the changes as part of the annual policy review.

Questions addressed in this paper

- What issues have been highlighted based on the review?
- What actions need to be undertaken to mitigate any issues identified?
- What changes to the Policy do we propose and why?
- What are the implications of these changes?

Conclusion

1. The whistleblowing process within Post Office is robust and the volume of whistleblowing reports received continues to rise year on year. Monthly MI is produced to track and monitor reports and investigations.
2. Further work is required to raise staff awareness, and this is being undertaken in conjunction with the People and Culture Director and a continuous awareness and improvement programme being delivered by the Financial Crime team.
3. The policy has been updated to reflect best practice recommended by Internal Audit, Legal review and feedback received from the staff survey conducted in March 2019.
4. Policy changes are minor and require no additional actions

Input Sought

The committee is asked to review the contents of this report, approve the updated Whistleblowing Policy and advise any further actions required.

POL00423568

The Report

Summary of activities relating to Whistleblowing reporting 2018-19

5. An internal audit of Whistleblowing was undertaken at the end of 2018 and concluded that *"The Whistleblowing process is well managed by the Financial Crime Team and monitoring and reporting has been improved since they assumed responsibility a year ago. The further improvements, both in progress and highlighted here, will help ensure that Post Office colleagues have confidence to use the process when appropriate".* There were three P2 and two P3 recommendations:
   - Minor amends and clarifications in the Whistleblowing Policy (para 10 below)
   - Expolink contract had not been renewed due to queries relating to GDPR clauses
   - A mechanism is needed to confirm staff awareness of whistleblowing arrangements and inform future awareness campaigns (para 3 and 18 below)
   - The Whistleblowing Policy states that investigations should be conducted in accordance with the Investigations Policy, however this had not been reviewed or updated since September 2016. Once the policy is updated, targeted training and guidance is needed for whistleblowing investigations.
   - Root cause analysis and action plans to address recurring cases was not fully evident – monthly MI and commentary has now been updated and implemented.
6. An online survey was undertaken in March 2019 to review staff awareness of Whistleblowing policy and reporting methods, and the findings from this are being incorporated into on-going training and awareness activity.
7. Monthly whistleblowing MI is produced and shared at regular meetings with HR representatives (Employee Relations and the People and Culture Director) to ensure consistent messages are being promoted. Additionally work is being undertaken with the People and Culture Director in relation to raising awareness of ethical behaviour in business.
8. The Financial Crime Team have attended various industry forums and Expolink Client Forums to understand industry best practice and enhancements that Post Office can introduce.
9. Whistleblowing reporting and investigation processes within the Financial Crime Team have been reviewed and enhanced.

Summary of Whistleblowing reports received 2018-19

10. Please see Appendix A for full reporting MI:
    - Year on year comparison shows that there has been an increase in whistleblowing reports from 37 in 2017/18 to 43 in 2018/19.
    - Most reports relate to individuals in our network – Postmasters and Agent Assistants as well as Post Office employees.
    - The most popular reporting channel continues to be the Speak Up line
    - The most common complaint relates to fraud and financial mismanagement. In most cases the allegations are against Postmasters or Agent Assistants
    - In 2018/19, there was an increase of reports with allegations of unethical behaviour or conduct and breach of internal policies and procedures

POL00423568

- A number of reports have been received from employees at one non-customer facing location, and HR are investigating if there are any underlying route causes or issues at this location.

Why do we need to review the Whistleblowing Policy?

11. The Policy was last reviewed and approved by the RCC in July 2018. The terms of the Policy require it be reviewed annually.

What changes to the Policy do we propose and why?

What are the key features that we propose and why?

12. There have been no legislation changes in the past year, but see Appendix B for a summary of the EU Whistleblowing Directive that the UK is expected to adopt by May 2021. Key impacts for Post Office include:

- Expansion of the definition of a whistleblower to encompass not only employees but also shareholders, volunteers, job applicants, non-executive directors, self-employed workers and contractors.
- A tiered reporting mechanism across all industry sectors and within both private companies and public institutions with 3 or 6 month response timeframes.
- A framework for protection against dismissal and other forms of retaliation from an employer against a whistleblowing employee

13. Minor policy amends have been made in relation to:

- Re-ordering content to provide clarity to readers in line with feedback received and incorporating clarification provided from legal review
- Updated contact details for external reporting and change of name of Public Concern at Work (PCAW) to 'Protect'
- Clarification that any so-called 'gagging clauses' in settlement agreements do not prevent colleagues from making disclosures in the public interest
- Method and type of feedback that a whistleblower can expect to receive
- Explanation that anonymous whistleblowers will not ordinarily be able to receive feedback and that any action taken to look into a report could be limited
- An indication of the time frame for investigating and responding to reports raised
- Clarification that the whistleblower does not need to provide evidence in order for the report to be investigated.

How did we develop these recommendations?

14. Reviewing policy queries and issues that have arisen over the previous 12 months and the internal audit recommendations.

What are the implications of these changes?

What will we need to do and by when, to implement and embed these Policy changes?

15. No material changes are required to comply with this updated Policy.

16. The Financial Crime Team monitor adherence to the minimum control standards set out in the Policy on an on-going basis through their whistleblowing reports and issues. Any control gaps identified will be reported to the RCC as required (see Appendix C for latest assurance status).

What will the impact be on our wider business?

17. Transparency of Post Office's adherence and commitment to the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998

POL00423568

What would the impact be of delaying approval?

18. Risk that the group breaches the Employment Rights Act 1996 and the Public Interest Disclosure Act 1998 by not having up to date policies and procedures to provide protections to whistleblowers.
19. Post Office Limited is required to maintain up to date policies to support contractual requirements with clients and suppliers (e.g. MoneyGram and the Partner Banking Framework) and failure to do so may result in a breach of contract, and whilst not material, could have commercial and reputational impacts.
20. Post Office Limited provides Post Office Management Services (POMS) with its policies suite in the form of "Group Policies". POMS is required under its regulatory responsibility to the Financial Conduct Authority to have up to date policies and failure to do so may lead to regulatory sanctions or penalties.

Activities planned for 2019-20:

21. In 2018-19, we shared posters, 3 intranet articles and a whistleblowing survey with employees.
22. The following activity is planned:
    - Explore running awareness campaigns via screen savers.
    - Review current employee induction process
    - Publish FAQs on the intranet and promote through One news article.
    - Promoting success stories, where possible.
    - Explore development of a short animation about Whistleblowing.
    - Enhance investigation training and procedures to include when and how whistleblowers are contacted
    - NAVEX Global (formerly Expolink Europe Ltd) contract renewal to be finalised.
    - Continuous collaboration with HR representatives (Employee Relations and the People and Culture Director) to ensure a consistent messages are being promoted and support the development of Post Office Ethical Values.
    - Conduct research into the possibility of rebranding the Speak Up/Whistleblowing service and alternative ways of promoting the service (e.g. short animations or videos).
23. On approval of the Policy amends, there will be a One communication to advise all employees of the changes and provide a link to the updated document on the Post Office Intranet.

Sally Smith
MLRO & Head of Financial Crime
27th June 2019

POL00423568

GROUP POLICIES

Whistleblowing Policy

9.2

Version – V3.2

Chief Executive's Endorsement

The Post Office Group is committed to doing things correctly. Our Values and Behaviours represent the conduct we expect. This Policy supports these to help us ensure that colleagues know how to report concerns regarding wrongdoing or dangerous practices and that they can do so without fear of recrimination.

POL00423568

1. Overview 3
1.1. Introduction by the Policy Owner 3
1.2. Purpose 3
1.3. Core Principles 3
1.4. Application 43
1.5. Legislation 4
1.6. What is Whistleblowing 4
1.7. Protecting the whistleblower ..... Error! Bookmark not defined.4
1.8. Whistleblowing Officer and 'Speak Up' ..... Error! Bookmark not defined.5
1.9. External Disclosures 65
2. Risk Appetite and Minimum Control Standards 87
2.1. Risk Appetite 87
2.2. Policy Framework 87
2.3. Who Must Comply? 87
2.4. Minimum Control Standards 98
3. Definitions 1413
3.1. Definitions 1413
4. Where to go for help 1514
4.1. Additional Policies 1514
4.2. How to raise a concern 1514
4.3. Who to contact for more information 1514
5. Governance 1615
5.1. Governance Responsibilities 1615
6. Control 1716
6.1. Policy Version 1716
6.2. Policy Approval 1716
Company Details 1716

9.2

POL00423568

1. Overview

1.1. Introduction by the Policy Owner

The General Counsel has overall accountability to the Board of Directors for the implementation of controls ensuring Post Office meets it Whistleblowing obligations. Whistleblowing is an agenda item for the Audit and Risk Committee and the Post Office board is updated as required.

1.2. Purpose

This Policy has been established to set the minimum operating standards relating to the management of Whistleblowing throughout the Group[1]. It is one of a set of policies which provide a clear risk and governance framework and an effective system of internal control for the management of risk across the Group. Compliance with these policies supports the Group in meeting its business objectives and to balance the needs of shareholders, ~~employees~~staff[2] and other stakeholders.

Commented [SS1]: Definition amended following legal review – see footnote 1

Commented [SS2]: Definition amended following legal review – see footnote 2

1.3. Core Principles

"Whistleblowing" refers to the act of exposing potential or actual wrongdoing and/or dangerous practices by reporting it either internally within an organisation, or to an external party. A whistleblower is a person who raises a genuine concern in relation to any wrongdoing, this includes criminal activity, regulatory breaches, miscarriages of justice, damage to the environment, financial impropriety, reputational damage, any breach of legal or professional obligations, dangers to health and safety and the deliberate attempt to conceal it. ~~Whistleblowing is the reporting of suspected wrongdoing and/or dangerous practices within Post Office. This would include serious accidents, bribery, fraud, any criminal activity, regulatory breaches, miscarriages of justice, health and safety risks, damage to the environment, financial impropriety, reputational damage and/or any breach of legal or professional obligations.~~

In order to encourage Whistleblowing and provide appropriate protections to whistleblowers, the governance arrangements described in this Policy are based upon the following core principles:

- To encourage the reporting of any concerns as soon as possible in the knowledge that Post Office will take all concerns ~~will be taken~~raised seriously and investigate fullyd, and that the confidentiality of all individuals will be respected;
- To provide guidance as to how to raise those concerns;
- To provide whistleblowers reassurance that all genuine concerns are raised without fear of reprisals, even if they turn out to be mistaken;

9.2

[1] In this Policy "Post Office" and "Group" mean Post Office Limited and any wholly owned subsidiary~~Post Office Management Services Limited~~.

[2] ~~In this Policy "employee" means permanent staff, temporary including agency staff, contractors, consultants and anyone else working for or on behalf of Post Office.~~ In this Policy "staff" means POL or Group's permanent, temporary and fixed term employees, workers including temporary workers, agency workers (where the terms on which they are engaged are not substantially determined by them), contractors, consultants and anyone else working under a contract with Post Office, in all cases having regard to s.230(3) and s. 43K ERA 1996.

Formatted: Indent: Left: 0", Hanging: 0.1"

POL00423568

- Post Office is committed to and oversees the implementation of the Policy in line with the Group's risk appetite. The Policy and associated procedures (set out or referred to in this document) are proportionate to the risks and complexity of the Group;
- Post Office undertakes a training and awareness program to ensure employees are aware of the Whistleblowing policy and procedure.

1.4. Application

Commented [SS3]: Section amended following legal review, particularly in relation to reports from non-employees

This Policy is applicable to all ~~employees~~ staff within the Group and outlines the manner in which Post Office will encourage, receive and investigate incidents of whistleblowing and the protections provided for whistleblowers by law.

In order to encourage reporting of wrongdoing, Post Office will, where appropriate, and to the extent possible, follow~~extend~~ equivalent principles to encourage, receive and investigate incidents of whistleblowing by~~protection to~~ Postmasters, Agent Assistants, and members of the public and will not subject any such persons to any detriment (including the termination of any contract or relationship with Post Office) for raising a genuine whistleblowing concern in an appropriate manner.

1.5. Legislation

The Group seeks to comply with all relevant UK legal and regulatory requirements including (but not limited to) the following legislation as amended or supplemented from time to time:

- Employment Rights Act 1996
- Public Interest Disclosure Act 1998

9.2

1.6. Protecting the Whistleblower (Your Legal Rights)

Commented [SS4]: Section amended generally following legal review and recommendations from Internal Audit

Post Office has a statutory obligation to protect whistleblowers and will support any individual person who raises genuine concerns under this Policy in an appropriate manner, even if they turn out to be mistaken. In respect of a certain class of person (broadly "staff" as defined under this policy) Post Office has a statutory obligation not to subject such persons to detriment or to dismiss them for whistleblowing.

Where a member of staff is subject to a Post Office settlement agreement, any clauses within it will not prevent the member of staff from whistleblowing. This should in any event be made clear by the terms of the settlement agreement itself and staff should receive independent advice in relation to those terms when entering into a settlement agreement.

Post Office will, at all times, respect the confidentiality and protecte the whistleblower's identity, however:

- It may be necessary in the course of an investigation to share this information with a relevant stakeholder (e.g. an investigator).
- There is no requirement for a whistleblower to provide personal contact information, but not providing this information may reduce Post Office's ability to undertake a thorough investigation into the concerns raised.

Post Office will take all reasonable steps to ensure that whistleblowers do not suffer any detrimental treatment as a result of raising a genuine concern in an appropriate manner. Detrimental treatment includes disciplinary action, dismissal, threats or other unfavourable treatment connected with raising a concern. Serious action, typically

POL00423568

disciplinary action, is likely to be be taken against any individual who threatens or retaliates against whistleblowers in any way.

If a whistleblower believes that they have suffered any such treatment, they should inform the Whistleblowing Officer immediately. The Whistleblowing Officer should take steps to address any victimisation, which may include working with the HR team to put appropriate measures in place. If the matter is not addressed the whistleblower (where they are staff) should raise it formally using Post Office's Grievance procedure.

In all cases the whistleblower's concerns will be treated sensitively and in confidence.

1.7 The Whistleblowing Officer

Post Office has appointed the General Counsel as the Whistleblowing Officer who can be contacted on whistleblowing GRO

The role of the Whistleblowing Officer is to receive all internal reports raised, regardless of the channel used, review any concerns raised and determine the best course of action, if any. They may ask for further information in order to make this decision.

The Whistleblowing Officer is also responsible for ensuring that reports are investigated and responded to in a timely manner. They are responsible for determining the appropriate parties who shouldto investigate the allegations raised, taking into account the sensitivities and seriousness of the report and the need to protect the whistleblower.

The Whistleblowing Officer is also responsible for identifying key trends or issues, and providing assurance to the Board that the policy is complied with.

1.8 How to Report Whistleblowing

Post Office supports and promotes a number of ways to provide reporting mechanisms:

- Direct to the Whistleblowing Officer GRO
- Via a complaint to a front line team, e.g. customer complaints, NBSC and Grapevine. These may be verbal or written communications.
- Contacting the "Speak Up" line, a confidential reporting service which is run by an independent company NAVEX Global (formerly Expolink Europe Ltd)

Contact details for the Speak Up line are:

- GRO
- https://wrs.expolink.co.uk/postoffice which is a secure on-line web portal

What should be rReported?
Whistleblowers should raise a concern if they are aware of, or suspect, certain wrongdoing which affects others (e.g. customers, members of the public, colleagues or the Post Office). The following lists some examples (this is a non-exhaustive list) of situations where an individual may raise a concern:

- Where Post Office or the Group is in breach of any legal obligation to which it is subject (usually a statutory rather than a contractual legal obligation)
- Financial Crime including Fraud, Money Laundering and financing of terrorism,
- Giving, offering or taking of bribes,
- Financial mismanagement, Tax evasion and Misreporting
- Racial, sexual, disability or other discrimination (Improper Behaviour) ,
- Practices that could put individuals or the environment at risk,
- Breach of Post Office internal policies and procedures

Commented [SS5]: Added following legal review

9.2

POL00423568

- Concerns about slavery or human trafficking[3], and
- Any conduct likely to damage Post Office's reputation

This policy should not be used by staff wishing to raise complaints relating to their own personal circumstances, such as the way they have been treated at work. Grievances and matters such as bullying and harassment should be raised in accordance with the procedures set out in the appropriate HR policy.

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

1.9 Responding to Whistleblowing Reports

In all instances any whistleblowing reports, regardless of reporting method, will be responded to within 5 working days and passed onto the Whistleblowing Officer.

All reports will be fully reviewed and investigated and any information, including emails, or records of telephone calls, letters, or any other form of communication stored securely and confidentially.

Commented [SS6]: Added for clarity from Internal Audit recommendation

The time frame for investigating the reports raised is dependent on the nature of the report and the investigation required, however, the whistleblower will be given feedback via the reporting channel they have used, or have given the Whistleblowing Officer permission to use (Speak Up line, e-mail or phone call) during the investigation and once it has been concluded.

The whistleblower may be kept informed of any action taken, however, this information may be limited if it is required to keep the confidence of other people.

Where a report received is anonymous, whistleblowers will not ordinarily be able to receive feedback and details of action ~~any action taken to look into a report by~~taken by Post Office may be limited.

9.2

1.10 External Disclosures

The aim of this Policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases individuals should not find it necessary to alert anyone externally.

However, the law recognises that in some circumstances it may be appropriate for individuals to report their concerns to an external body such as a regulator. It will rarely, if ever, be appropriate to alert the media at least without informing Post Office or an external agency first and usually in that order.

Commented [SS7]: Added following legal review

We strongly encourage individuals to seek advice before reporting a concern to anyone external. The independent Whistleblowing charity, Protect (formerly Public Concern at Work) have a list of prescribed regulators for reporting certain types of concerns. Their contact details are as follows:

Helpline: GRO
~~E-mail: whistle~~ GRO

[3] More information in relation to Modern Slavery can be found here - http://corporate.postoffice.co.uk/slaverystatement

POL00423568

Website: ~~-~~www.pcaw.org.uk/advice-line/~~co.uk~~

~~Public Concern at Work~~Protect operates free, confidential advice to people concerned about crime, danger or wrongdoing in the workplace. ~~-~~All Protect advisors are legally trained and supervised by qualified lawyers and their advice is fully confidential and subject to legal privilege. All information, including emails, or records of telephone calls, letters, or any other form of communication with Protect advisors is stored in a fully encrypted format.

Post Office Money Services (POMS) is directly regulated by the Financial Conduct Authority (FCA), Post Office Limited is an appointed representative of Bank of Ireland (UK) Limited. As such individuals may decide to whistleblow directly to the FCA, and can do so by using one of the following channels.

Helpline: GRO
E-mail: whistle GRO
Website: www.fca.org.uk/site-info/contact/whistleblowing
Address: Intelligence Department (Ref PIDA), Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN~~Intelligence Department (Ref IDA), Financial Conduct Authority, 25 the North Colonnade, London E14 5HS~~
Whistleblowing concerns usually relate to the conduct of our staff, but they may sometimes relate to the actions of a third party, such as a customer, supplier, agent, Postmaster or service provider. In some circumstances the law will protect individuals if they raise the matter with the third party directly. However, we encourage individuals to report such concerns internally in the first instance.

Commented [SS8]: Updated contact details

Commented [SS9]: Updated information from Protect website

Commented [SS10]: Updated contact details

Commented [SS11]: Added following legal review

9.2

POL00423568

2. Risk Appetite and Minimum Control Standards

2.1. Risk Appetite

Risk Appetite is the extent to which the Group will accept that a risk might happen in pursuit of day to day businesses transactions. It therefore defines the boundaries of activity and levels of exposure that the Group are willing and able to tolerate.

The Group takes its legal and regulatory responsibilities seriously and consequently has[4]:

- **Tolerant risk appetite** for Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality
- **Averse risk appetite** for litigation in relation to high profile cases/issues
- **Averse risk appetite** for ligation in relation to Financial Services matters
- **Averse risk appetite** for not complying with law and regulations or deviation from business' conduct standards for financial crime to occur within any part of the organisation
- **Averse Risk Appetite** in relation to unethical behaviour by our staff.

The Group acknowledges however that in certain scenarios even after extensive controls have been implemented an action may still sit outside the agreed Risk Appetite.

2.2. Policy Framework

Post Office has established a suite of policies and procedures, on a risk sensitive approach which are subject to an annual review. The policy suite is designed to comply with applicable legislation and regulation. The Whistleblowing Policy should be considered and read in conjunction with other policies where relevant. These may include the Financial Crime Policy, the Anti-Bribery & Corruption Policy, Health & Safety Policies and HR Policies where relevant.

2.3. Who Must Comply?

All third parties who do business with the Group, including consultants, suppliers and business and franchise partners, will be required to agree contractually to this policy or have their own equivalent policy.

Any investigations will be carried out in accordance with the Investigations Policy which is available on the Post Office Intranet

[4] The Risk appetite was agreed by the Groups Board January 2015

POL00423568

2.4. Minimum Control Standards

A minimum control standard is an activity which must be in place in order to manage the risks so they remain within the defined Risk Appetite statements. There must be mechanisms in place within each impacted business unit to demonstrate compliance. The minimum control standards can cover a range of control types, i.e. directive, detective, corrective and preventive which are required to ensure risks are managed to an acceptable level and within the defined Risk Appetite.

The table below sets out the relationships between identified risk and the required minimum control standards in consideration of the stated risk appetite. The subsequent pages define the terms used in greater detail:

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Receipt and investigation of whistleblowing reports	Failure to meet legal and regulatory requirements	Directive Control: Post Office must nominate a Whistleblowing Officer to receive reports, ensure that all reports are fully investigated and that any appropriate corrective action is undertaken.	Post Office CEO and Board	Ongoing
		The Whistleblowing Officer must provide a whistleblowing report to the R&CC and ARC at least annually.	Whistleblowing Officer	Annually
		Any serious whistleblowing concerns must be promptly escalated to the Chairman of the Post Office Audit and Risk Committee.	Whistleblowing Officer	Ongoing
		Preventative Control: All employees are trained and the policy is available to them	Whistleblowing Officer	Training must be provided at least annually

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		The Whistleblowing Officer must ensure that appropriate arrangements are in place to ensure that whistleblowing reports are addressed promptly including during absences	Whistleblowing Officer	Ongoing
		Communications and awareness provided to all employees and Policy document published on the Intranet.	Head of Financial Crime	Annually
Breach of confidentiality	Failure to ensure confidentiality for the whistleblower	Preventative Control: Whistleblowing Policy	Whistleblowing Officer	Ongoing
		Confidential Speak Up line reports are shared only with the Whistleblowing Officer and nominated deputies	Whistleblowing Officer	Ongoing
		Whistleblowing email ~~inbox with access~~inbox access is restricted to the Whistleblowing Officer and nominated deputies	Whistleblowing Officer	Ongoing
		Whistleblowing Officer must put arrangement in place to protect the confidentiality of the whistleblower during investigations	Whistleblowing Officer	Ongoing
		Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to review and take necessary actions.	Whistleblowing Officer	Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
Incorrect handling of whistleblowing report	An individual may raise a whistleblowing report with other individuals in the Group. Details may then be shared with various stakeholders before being passed onto the Whistleblowing Officer	Preventative Control: Training provided to contact teams to identify potential whistleblowing reports and ensure these are correctly handled, e.g.: • Grapevine, • NBSC, • Customer Support, and • Executive Correspondence Team. Communications and awareness provided to all employees and Policy document published on the Intranet. Corrective Control: All incidents of breaches are escalated to the Whistleblowing Officer to investigate and take appropriate actions.	Whistleblowing Officer Head of Financial Crime Whistleblowing Officer	Annually Annually Ongoing
Insufficient Information	Failure to capture/report sufficient information about the issue may mean that the underlying issue cannot be properly investigated and resolved	Directive Control: Individuals are encouraged to report issues and provide full information and their contact details, where they feel able to do so Corrective Control: All reports, including those where insufficient information has been provided and no further action was taken are recorded on the Whistleblowing	Whistleblowing Officer Whistleblowing Officer	Ongoing Ongoing

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		database, which is reviewed for trends and issues.		
The 'Speak Up' Service	Failure to effectively record whistleblowing reports and pass onto the Whistleblowing Officer, due to factors such as resource or IT failure.	Preventative Control: The Whistleblowing Officer must review the effectiveness of the service provided by NAVEX Global~~Expolink Europe Ltd~~ (formerly known as ~~InTouch MCS Ltd~~Expolink Europe Ltd) at least annually The Whistleblowing Officer must review the effectiveness of the processes operated by each of Grapevine, NBSC, Customer Support, and The Executive Complaints Team at least annually to ensure that whistleblowing reports are identified and communicated promptly.	Whistleblowing Officer Whistleblowing Officer	Annually Annually
Treatment of Whistleblowers	Breach of whistleblowing guidelines such that a whistleblower suffers prejudice, detriment or dismissal as a result of making a whistle blowing report	Preventative Control Training must be provided to all people managers as part of their induction process as a manager and on appointment to Post Office Annual training must be provided to all Post Office staff to remind them of the protections available to whistleblowers and the	Whistleblowing Officer and HR Training Manager Whistleblowing Officer and HR Training Manager	Ongoing Ongoing

Commented [SS12]: Reflects change of name

POL00423568

Risk Area	Description of Risk	Minimum Control Standards	Who is responsible	When
		importance of identifying and reporting wrongdoing The Code of Business Standards must refer to the whistleblowing policy and must be provided to all new joiners as part of their induction programme.	Whistleblowing Officer and HR Training Manager	Ongoing

POL00423568

3. Definitions

3.1. Definitions

Grapevine
24/7 Security Support Centre provided by Kings Ltd. Grapevine provide security advice and record all security incidents across the business, this includes burglaries, robberies and the reporting of suspicious activity.

Telephone Number: GRO
E-mail: grapevine.admin GRO

NBSC
Network Business Support Centre (NBSC) is a helpline and the first port of call for Post Office branches if they have any operational query or require assistance.

Telephone Number: GRO
E-mail: nbscenquiries GRO

Customer Support Team
Complaints handling team based in Chesterfield. The team address complaints reported into Post Office via various channels, including post and telephone.

E-mail: customercare GRO

Executive ~~Complaints~~ Correspondence Team
This team handles all complaints addressed directly to the Group Executives. The team liaise with various stakeholders within the business in order to resolve complaints.

E-mail: flagcaseadvisor GRO

9.2

POL00423568

4. Where to go for help

4.1. Additional Policies

This Policy is one of a set of policies. The full set of policies can be found at:

https://poluk.sharepoint.com/sites/thehub/SitePages/Key%20policies.aspx?web=1

4.2. How to raise a concern

Any Post Office employee who suspects that there is a breach of this Policy should report this without any undue delay. Whistleblowing can be reported via the following channels:

- Their line manager,
- A senior member of the HR Team, or
- If either or both are not available, staff can contact the Post Office's Whistleblowing Officer, who can be contacted by email at: whistleblowing GRO or by telephone on: GRO
- Alternatively staff can use the Speak Up service available on GRO or via the secure on-line web portal: https://wrs.expolink.co.uk/postoffice

In some instances it may be appropriate for the individual to report in the form of a complaint to Grapevine, the Customer Support Team or the Executive Correspondence Team.

4.3. Who to contact for more information

If you need further information about this Policy or wish to report an issue in relation to this Policy, please contact the Policy sponsor or Policy owner.

Commented [VC13]: Should we rename this section as it is fairly similar to "1.8 How to Report Whistleblowing". Possible "How to report policy breaches?"

9.2

POL00423568

5. Governance

5.1. Governance Responsibilities

As at the date of approval of this Policy, the General Counsel is both the Policy Sponsor and Policy Owner, responsible for oversight of the Policy.

The Audit and Risk Committee are responsible for approving the Policy and overseeing compliance.

The Board is responsible for setting the Group's risk appetite.

POL00423568

6. Control

6.1. Policy Version

Date	Version	Updated by	Change Details
April 2016	1.4	Jane MacLeod	Sponsors review and sing-off
August 2017	1.5	Vitor Camara	Annual Review and update.
September 2017	1.6	Thomas Richmond	POL R&CC approval
September 2017	2	Thomas Richmond	Final version approved
June 2018	2.1	Vitor Camara	Annual review and update.
July 2018	2.2	Sally Smith	POL R&CC approval
July 2018	2.3	Sally Smith	POL ARC approval
September 2018	2.4	Sally Smith	POMS ARC approval
September 2018	3	Vitor Camara	Final Version approved
June 2019	3.1	Sally Smith	Annual review and update
June 2019	3.2	Sally Smith	Incorporating legal review comments

6.2. Policy Approval

Group Oversight Committee: Risk and Compliance Committee and Audit and Risk Committee

Committee	Date v. 3.0 Approved
POL R&CC	10th July 2018
POL ARC	31st July 2018
POMS ARC	20th September 2018
Committee	**Date Approved**
POL R&CC	
POL ARC	
POMS ARC	

Policy Sponsor: Group Director of Legal, ~~Risk~~ Compliance & Governance
Policy Owner: Whistleblowing Officer
Policy Author: Head of Financial Crime

Next review: July 2020

Company Details

Post Office Limited and Post Office Management Services Limited are registered in England and Wales. Registered numbers 2154540 and 08459718 respectively. Registered Office: Finsbury Dials, 20 Finsbury Street, London EC2Y 9AQ.

POL00423568

Post Office Management Services Limited is authorised and regulated by the Financial Conduct Authority (FCA), FRN 630318. Its Information Commissioners Office registration number is ZA090585.

Post Office Limited is authorised and regulated by Her Majesty's Revenue and Customs (HMRC), REF 12137104. Its Information Commissioners Office registration number is Z4866081.

POL00423568

Modern Slavery Act Statement

Author: James Scutt Sponsor: Amanda Jones Meeting date: 4th July 2019

Executive Summary

Context

The Modern Slavery Act 2015 (the Act) challenges slavery, domestic servitude, forced and compulsory labour and human trafficking. Post Office is required to produce an annual slavery and human trafficking statement (Statement) setting out what steps have been taken to ensure its business and supply chains are mitigating the risks of modern slavery. This paper attaches the third Statement which documents progress on our previous year's commitments and outlines the actions that we commit to take in the year ahead.

Questions addressed in this paper

1. Why do we need an updated Statement?
2. What are the key points to note about our Statement?
3. What are the implications for the board and the business?
4. Is the Post Office compliant with the Act?

Conclusion

In order to give Post Office an independent and balanced view of its compliance to the requirements of the Modern Slavery Act, we employed the services of an external body of expert consultants with particular skill and knowledge in Modern Slavery.

Overall the Post Office is compliant with the MS ACT 2015 in terms of its legal obligations. It has made progress in defining what needs to be done across the business and is beginning the longer term task of robust implementation.

- Post Office has prepared a new Statement for 2019/2020 in line with the Act. The Statement must be published on Post Office's website within 6 months of financial year end.
- The steering group has been meeting monthly, has made progress and will continue to evolve with a full review of its terms of reference going forward.
- Due to the lack of control over operations in this area, the highest level of risk continues to be within our Agency Network but we have also identified several more areas where proximity of brand also poses a risk for Post Office. (When the Post Office branding appears on retail packaging, sourced by one of its suppliers)
- Published company statements on modern slavery face scrutiny from the media, pressure groups and the public. As an organisation with a reputation of trust and

POL00423568

a stated social purpose, we consider it important for Post Office to demonstrate a clear commitment. Civil society would expect the Post Office to be a champion in this area because of this trust legacy.

- To be able to implement robust monitoring and due diligence, Post Office needs to increase the resources (people and budget) from what has been allocated to Modern Slavery to date and have someone sufficiently dedicated to overseeing the implementation across the business.

Proposed actions for 2019/20:

- Implement a new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.
- Review our supply base retrospectively by applying the focus of our new IT tracking system.
- Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.
- Continue to raise awareness of Modern Slavery across Post Office supply chain and branch network in both directly managed and agency branches.
- Deploy specific MS awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.
- Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.

Input Sought

The RCC IS asked to approve the 2018/2019 Statement and endorse the proposed actions for the business to take forward in the 2019/2020 financial year.

Input Received

We consulted all members of the MSA Steering Group which comprises of representatives across functions including Legal, Procurement, Risk, Employee Relations and Learning and Development as well as independent consultants.

The Report

Why do we need Modern Slavery Act Statement?

The requirement to publish a Statement applies to "commercial organisations" which (a) supply goods or services and (b) have a total turnover of not less than £36 million. It will therefore not apply directly to Postmasters if their annual turnover is less than £36 million. As Postmasters are part of the Post Office supply chain, Post Office must state what steps it has taken to ensure that it mitigates the risk of slavery and human trafficking in any of its supply chains or its business. Payzone has a turnover of just under the threshold so is not legally required to produce a separate MS Statement, best practice would be to do so and this is something we may want to consider. PZ will still be included as a business owned by the Post Office.

POL00423568

Post Office is required under s.54 of the Act to produce an annual slavery and human trafficking statement listing the steps taken to ensure its business and supply chains are slavery free. This paper attaches the third Statement (Appendix 1) which records what steps we have taken in 2018/2019 and outlines the actions we commit to take in 2019/2020. The Statement must be approved by the Post Office Board and signed by a Director.

What are the key points to note about our updated Modern Slavery Act Statement?

Our 2018/2019 statement records the progress we have made against those commitments and lists our commitments to tackle modern slavery across POL and POI for the financial year 2019/2020. The commitments were developed by the MSA Steering Group which includes representatives from Legal, Procurement, Risk, Employee Relations and Learning and Development. Our commitments are:

- Raise awareness of Modern Slavery across our supply base.
- Improve the due diligence assessment for onboarding new suppliers to our systems.
- Raise awareness of Modern Slavery across Post Office, its suppliers and within the agency network.
- Educate field teams out in the agency network on spotting the signs of Modern Slavery.
- Review our supply base and revise our supplier management processes.

In formulating our commitments for 2019/2020 we engaged subject matter experts, "Good Values" to fully review Post Office's exposure to risk and approach to MS.

Good Values are a leading corporate responsibility and sustainability consultancy with over 10 years' experience working globally with corporates, NGOs and government departments. They help organisations manage the risks and exploit the opportunities from social and sustainability issues.

The main areas of risk are highlighted as:

Public perception that where a Post Office fascia is in place that the facility is a Post Office and not an independent retailer that "includes" a Post Office service.

Risk by association that those working with a Post Office fascia but also operating other businesses, directly and indirectly associated with retail.

Challenging dialogue to have with consumers about trust and control of Postmasters if something goes wrong. Given the public perception is that the Post Office controls all places where there is a Post Office facia, stating in defence that: "We do not control them", "We did not know about this", "We have T&Cs that prohibit this", would not be good enough in the public domain, and there would be reputational damage.

POL00423568

Lack of Resource to be able to implement robust monitoring and due diligence, dedicated resources (people and budget) would need to be allocated to Modern Slavery to oversee the implementation across the business.

What are the implications for the board and the business?

A potential consequence of failing to show adequate progress on tackling modern slavery within the company statement is damage to reputation and brand.

Latest Government guidance on the Modern Slavery Act and expectations from civil society is for companies to show year on year progress on how they are tackling the risks of modern slavery within their operations and supply chain.

Our annual statement therefore has to show more than just a tick-box exercise and must demonstrate a material commitment to tackling the potential risk of modern slavery within the organisation.

We are confident that the detail in our 2018/2019 statement recording our progress on last year and our proposed actions for the financial year 2019/2020 are appropriate. We will monitor developments, and keep the adequacy of the Statement under review.

Is the Post Office compliant with the Act?

Overall the PO is compliant with the legal obligations of the MS Act.

To establish the level of monitoring and due diligence within the Post Office that would be expected by civil society and stand up to public scrutiny, further focus and resource is required. Overall the Post Office is compliant with the legal obligations of the MS ACT 2015. It has started to make progress within the business, but it has yet to: embed training with employees; address the risk evaluation of our Postmasters and Agency businesses; conduct the required level of mapping and risk assessment with suppliers as set out in the Statement.

POL00423568

Appendix 1

1. Modern Slavery Statement 2019/2020

MODERN SLAVERY ACT TRANSPARENCY STATEMENT 2019/20

Post Office Limited (Post Office) & Post Office Management Services Limited (POMS).

This statement is made pursuant to section 54(1) of the Act. It sets out the steps taken by Post Office & POMS during year ending 31st March 2019 to mitigate the risks of modern slavery and human trafficking in its business and supply chains.

Post Office and POMS are committed to combating the risk of modern slavery or human trafficking in our supply chain and business operations. We are committed to taking appropriate steps to ensure that everyone who works for Post Office in any capacity, benefits from a working environment in which their fundamental rights and freedoms are respected.

This is the third statement in which we report on our efforts to mitigate the risks of modern slavery in line with the requirements of the Act. Our history has seen us focus on the rights and wellbeing of the people who work for Post Office and for our suppliers for many years. Our statement provides details of our policies, our approach and the actions we have taken in the 2018/19 financial year to strengthen our programme and commitment to respect and uphold people's fundamental rights and freedoms.

OUR BUSINESS AND SUPPLY CHAIN

Post Office is the UK's largest retail network and the largest financial services chain in the UK. We have provided services for more than 370 years and currently supply a range of essential products and services to communities right across the UK.

Our UK Government mandate is to provide at least 11,500 Post Offices, some within certain geographical, demographic and social criteria that provide a unique operational challenge for Post Office compared to other wholly commercial retail or financial institutions. We are often at the heart of the local communities, some of which can be challenging environments to operate in.

Post Office directly controls around 2% of the Network of branches which consumers will generally recognise as the larger branches often situated in the centre of towns and cities across the UK. The remainder of the branches are managed on an agency basis by independent small retailers and shop owners operating Post Office services within their own store. Business owners may own more than one shop operating Post Office services and have a range of other non connected business interests. We also have agent managed facilities within some larger high street commercial partners, who like the smaller independent retailers, provide their own trained and friendly staff to provide our Post Office services to consumers.

POL00423568

Banking services

Post Office banking services are provided in Post Office branches on behalf of the customers of UK banks.

Postmasters

Postmasters can operate one or more branches. As agents they have full control over how their branches within their retail premises are run on a daily basis. All those working in an agency Post Office branch are employed directly by the retailer. The Retailer is self-employed and typically takes on a Post Office as a valuable community service provided within their own retail business. Post office has no direct control over the operation of these independent SME businesses but does have the ability to influence and inform. Post Office aims to support Postmasters with their Post Office operations and influence their behaviours.

Commercial partners

A large proportion of the agency network is managed by commercial partners – corporate retail organisations with familiar fascia brands who themselves have a multiple number of high street stores.

Trade Unions

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

Third Party Suppliers

We also procure products and services from a range of managed suppliers, ranging from small and medium enterprises to large multinationals. Purchasing for our own managed Post Offices is controlled centrally by the Procurement team who also set the Supplier Relationship Management standards to ensure our teams maintain a consistent approach to supplier management.

OUR BELIEFS AND PRINCIPLES

Respect for the dignity of the individual and the importance of each individual's human rights form the basis of the behaviours we expect in every workplace and are communicated through our Code of Business Standards. We will not accept any form of discrimination, bullying or harassment. We require all our managers to implement policies designed to ensure equality of opportunity and inclusion for all Post Office employees.

POL00423568

OUR POLICIES

We operate a number of policies to ensure we are conducting business in an ethical and transparent manner. These include:

CODE OF BUSINESS STANDARDS

We have a Code of Business Standards which underpins everything we do. The Code is mandatory and extends to everyone directly employed by Post Office. It requires all of us to act ethically and comply with legal requirements at all times, putting our principles into practice in everything we do. The Code of Business Standards was updated during the 2017 financial year to include references to Modern Slavery.

WHISTLEBLOWING

We operate a Whistleblowing Policy so that all Post Office employees know how to raise concerns regarding wrongdoing or dangerous practices. The policy was updated during the 2017 financial year to include references to concerns about Modern Slavery.

There are a number of ways people can report any concerns regarding slavery or human trafficking within Post Office, by either contacting the Whistleblowing Officer or via our anonymous external confidential reporting service 'Speak Up' which is regularly communicated to all employees, suppliers and contractors. This is overseen by our General Counsel (Whistleblowing Officer). Every report submitted is assessed and investigated.

RECRUITMENT & ONBOARDING POLICY

Our recruitment and on-boarding policy for Post Office employees sets out the overarching principles and controls to be followed and applied to ensure that personnel resourcing is conducted in a fair, open and transparent manner, including conducting eligibility to work in the UK checks for all employees.

DUE DILLIGENCE PROCEDURES IN RELATION TO SLAVERY AND HUMAN TRAFFICKING IN OUR BUSINESS AND SUPPLY CHAIN.

Post Office/POMS employs solely within the UK.

Our recruitment procedures ensure that all prospective employees are legally entitled to work in the UK. All successful applicants must produce, on their first day, one of the following: their original passport, driving license or birth certificate. Additionally, to comply with the Asylum and Immigration Act 1996 requirements, if they are from a non-European Economic Area (EEA) country, evidence of a right to reside and work in the UK must be produced.

We carry out reasonable and practical due diligence in the sourcing of goods and services and ensuring that the Act's obligations form part of the procurement process. As part of this process we have conducted a review of the criteria used by Post Office

POL00423568

to evaluate whether suppliers meet Post Office's minimum tendering requirements. We have also reviewed our standard form procurement contracts to ensure that they make explicit reference to the Act, as well as covering other areas of company information, policies and procedures. This enables the procurement team to assist Business Units to identify and assess any potential risks relating to the goods or services being procured.

IDENTIFYING, ASSESSING AND MANAGING RISK

WHERE ARE THE RISKS OF MODERN SLAVERY AT POST OFFICE/POMS

Post Office understands that our procurement of goods and services from third parties carry with it the risk of modern slavery and human trafficking.

We understand that a potential for risk of modern slavery sits within our agency network as there are a large number of people employed by independent retailers acting as Postmasters (including commercial partners) who are not direct employees of Post Office or POMS.

GOVERNANCE

We have a cross-functional steering group through which we develop and coordinate our approach to addressing modern slavery risks within our operations and supply chain. This group consists of expertise from the legal, procurement, compliance and operational functions in Post Office.

TRAINING

We provide annual Compliance Awareness Training to all our employees and postmasters, which is tailored to ensure an appropriate level of understanding of issues such as modern slavery and the Act's requirements.

WHAT DID WE DO THIS YEAR

Proposals from 2018 Statement	**Progress on 2018 proposals**
Improve the due diligence assessment for onboarding new suppliers to our systems	We carried out a detailed assessment of our new supplier on-boarding process and identified a number of recommendations which will help ensure a robust assessment of new suppliers and their ways of working.
Review our supply base and revise our supplier management processes	We have designed an enhanced process and detailed content to be included in new system described above. Our CSR questionnaire is being trialled with a small cross section of suppliers, to test, review and make improvements to the question format, evaluation process and feedback/ improvement plan.

POL00423568

	We have aligned this with Post Office Compliance and Audit functions who conduct physical audits of Supply Chain suppliers. This ensures maximum benefit from our efforts and no duplication, or overburdening of the suppliers.
Raise awareness of Modern Slavery across our supply base	We created our Supplier Code of Conduct and published it on our public website. http://corporate.postoffice.co.uk/our-suppliers This Code of Conduct is used in the on-boarding process and other procurement exercises. Depending on the outcomes of the CSR questionnaire, we will devise additional awareness material as appropriate and distribute to our suppliers proactively.
Raise awareness of Modern Slavery across Post Office, its suppliers and within the agency network.	We issued guidance and Modern Slavery awareness raising material for Postmasters through our branch Network management teams and communication channels.
Educate field teams out in the agency network on spotting signs of Modern Slavery.	We sourced best practice training and awareness materials from suppliers and developed it to align and resonate with our Branch network management field teams. We will start to roll this training out to frontline staff.

WHAT COMMITMENTS ARE WE MAKING TO TACKLE MODERN SLAVERY IN THE YEAR AHEAD

As part of our initiative to identify and mitigate risk throughout 2019/20 we are committed to:

- Implement our new IT system to track and monitor the on-boarding of new suppliers, ensuring a robust assessment and oversight of their ways of working and risk profile around Modern Slavery.
- Review our supply base retrospectively by applying the focus of our new IT tracking system.
- Raise awareness of Modern Slavery across our existing suppliers where they are found to be lacking focus.
- Continue to raise awareness of Modern Slavery across Post Office branch network across both directly managed and agency branches.
- Deploy specific MS awareness training to our field teams to enable them to robustly spot signs of Modern Slavery.
- Review the guidance given to Postmasters to ensure alignment with wider business activity and network support teams.

POL00423568

REMEDIATION PROCESSES

If you have any concerns about the issues raised in this statement or if you think you have identified signs of Modern Slavery then please contact us on the below contacts:

Post Office's Whistleblowing Officer: whistleblowing GRO or by telephone on: GRO
The Government's Modern Slavery Helpline on GRO

We encourage any individual who has concerns about unethical behaviour in any part of our business or operations to speak up and to do so without fear of retaliation. We will review all instances of non-compliance, on a case-by-case basis and will implement appropriate remedial action.

REVIEW

This statement shall be reviewed and published annually.

POL00423568

UK Data Protection Act (incorporating GDPR) Compliance Status Report

Authors: Chris Russell Clare Hammond Sponsor: Ben Foat Meeting date: 4th July 2019

Executive Summary

Context

- The UK Data Protection Act 2018 (UK DPA 18) came into force in May 2018 incorporating the EU General Data Protection Regulations (GDPR) along with UK specific exemptions and interpretations. The legislation builds on the 1998 DPA and includes increased penalties for non-compliance (up to 4% of global annual turnover) and a requirement that organisations demonstrate accountability.
- The Information Commissioner's Office (ICO) is the UK Data Protection Authority, which enforces the UK DPA 18 and regulates Post Office.
- Post Office processes personal data in a uniquely complex environment. Information is processed on behalf of more than 140 different data controllers, including banks and government agencies. In turn, Post Office uses more than 170 different data processors, who process personal data on behalf of Post Office.
- In order to meet the GDPR and DPA requirements, the GDPR Programme was set up in 2017 and ran to April 2019. The programme looked across the Post Office Group, excluding Payzone.
- The programme was tasked to achieve 'effective compliance'[1] by May 2018 and 'substantive compliance'[2] April 2019.
- This paper is an assessment by the Data Protection Team of the level of compliance achieved by the GDPR Programme and highlight the actions that need to be taken to maintain the achieved Compliance levels.

10

Questions this paper addresses

- What level of compliance with the UK DPA 18 has Post Office achieved through the GDPR programme and is this within Post Office's risk appetite?
- What further actions are needed to ensure that Post Office achieves and sustains the required level of compliance?
- What structures are in place to monitor, improve and report compliance to the UK DPA 18 in a 'business as usual' setting?

[1] *Covering aspects visible to data subjects such as Marketing Permissions and Privacy Notices*
[2] *Covering other data issues such as Process Mapping and Information Rights*

POL00423568

Conclusion

1. The GDPR Programmes established appropriate controls, from which Post Office can reasonably derive a high degree of confidence that its operational process are compliant.
2. There is still work to be done to implement further administrative controls, with particular focus in the following areas, which are being delivered through separate projects and as part of remediation work by the Data Protection Team and relevant businesses:
    a. Contract Remediation
    b. Records Retention
    c. Data Classification
    d. Data Storage.
3. The Data Protection team is confident that the necessary remediation plans are in progress to deliver confidence in our compliance maturity.
4. Additionally, there are two key areas that require the Data Protection Team's focus:
    a. Refining Data Protection governance and setting up audit and review processes by end September 2019
    b. Third party risk and monitoring of new operational practices review with the aim of moving to a more robust position by the end of 2019.
5. Lastly, in order to support the businesses in managing data compliantly, we have proposed establishing a quarterly "Privacy Forum".

Input Sought

The Committee is asked to note the Data Protection team's compliance findings and is requested to support the proposals included in this paper.

POL00423568

Report

What level of compliance with the UK DPA 18 has Post Office achieved through the GDPR programme and is this within Post Office's risk appetite?

1. Approximately 575 different processing activities have been identified and mapped as part of the GDPR Programme. Where appropriate, and to help explain complex processes, data flow diagrams have been produced and all are inventoried within our One Trust Privacy Management record system.
2. These processes encompass all current areas in Post Office (excluding Payzone) where Personal Data is used.
3. A thorough review was undertaken and all processes, with the exception of Record Retention, are compliant with the provisions of the UK DPA18 and are within Post Office Risk Appetite.
4. However, we have identified discrepancies between the processes, which are compliant, and elements of Post Office policies (such as Data Classification, Data Storage and Legitimate Interest Assessment). As a result there is an ongoing remediation exercise in place between the Data Protection team and process owners to gain alignment with a targeted completion date of December 19
5. The GDPR programme also included amending key contracts to ensure they are compliant with the new legislation. To date some 450 have been completed, with a further 150 currently being reviewed/to start review. This work will continue throughout 2019/20, with the Data team working alongside Legal. This is a low risk to Post Office as remediation was prioritised at the Material and high risk contracts. The majority of those not remediated are Non-Material IT Service Contracts.
6. Privacy Notices are in place for all key groups of data subjects. There remain some gaps, in particular, how to deliver information to customers in Branch. A regular review and sign off process will be established by the end of September 19 to ensure that all Privacy Notices are in line with ICO guidance.
7. A robust annual training course that all staff are required to take has been rolled out but we are developing further awareness materials and regular communications with the Training and Communications teams to reinforce this. We will also assess the benefits of holding an annual "Privacy Day" to highlight the importance of data privacy both at work and also in our personal lives.
8. The GDPR programme has significantly improved Post Office's compliance. Further work remains to be done but there is now a low risk of sanction for not amending processes etc. from the regulator. The programme prioritised remediation on operational controls where a failure in this area would attract regulatory scrutiny.

Improving ongoing compliance across Post Office?

9. Governance structures, including the establishment of a regular Privacy Forum with terms of reference, need to be defined and implemented by the end of Sept

POL00423568

19. Key management information within a dashboard are planned to be available to internal stakeholders on a monthly basis and reported to the Forum quarterly.

10. The Data Protection Team will work with the Policy Governance manager to develop good accountability and governance structures so that ownership of policies, processes, contracts and assets is well defined and responsibilities understood throughout the organisation.

11. It is proposed that we establish a network of 'data privacy champions' throughout the organisation by the end of Dec 19. The face to face GDPR training that was undertaken in 2018 demonstrated that there are a number of individuals who have a keen interest in the topic and would like to be a key contact for their area of the business

12. Further remediation work will be conducted over the next year to ensure adequate controls are in place for the processing of 'unstructured data' (outside the scope of the GDPR Programme). The Process Mapping exercise identified that Unstructured Data is Personal Data that is being stored outside of its source system, for example data held in Outlook or local drives on laptops and PC's. This will tie in with the Records Retention project with targeted completion of July 20

13. The storage of this unstructured data is **NOT** in contravention of the UK DPA18 but is outside of Post Office policy. Therefore, through education, awareness and remediation workshops this unstructured data will be stored correctly with the adequate controls being developed.

14. An example of these controls has been developed and implemented within HR Reports. Since September last year requests for release of raw HR Personal Data have to be validated and verified by the Data Protection team prior to release to the business. There are no exceptions to this process.

Plans to improve Post Office Data Protection Review procedures?

15. A review of Data Protection has been included in the 2019/20 Internal Audit plan. The objective of this review is to assess the operational effectiveness of the structure, process and controls in place to ensure ongoing GDPR compliance. In addition Internal Audit will follow up the actions from the 2017/18 GDPR programme review to ensure those controls are embedded and sustainable.

16. The Data Protection Team will conducting a programme of informal 'Privacy Reviews' and walk-throughs targeting key areas of the business that will commence in Q4 2019. This will be risk based and could be as a result of an incident (or series of regular low level incidents) or target groups who process particularly sensitive personal data.

17. The Third Party Risk Assessment process is established and focusses on the IT Security of key vendors. The Risk team has agreed to include Data Protection as part of the reviews and assessments. In addition, an ongoing due diligence process should be established by Mar 2020 that requires higher risk processors to regularly report their compliance status and to demonstrate adherence to key contractual terms.

18. Data Protection by Design processes will be evaluated to identify enhancements that can be made to ensure that Data Protection is considered and built into every stage of a product or process development. The Data Protection team has made significant progress by building more effective working relationships with the

POL00423568

business teams. However this requires formalising and documenting, particularly as the organisation embraces Agile ways of working.

19. Complaint and enquiry handling from data subjects, particularly customers, has improved and is handled and tracked. However, enhancements are planned to be implemented by Nov 2019 to ensure that the processes are repeatable and measurable. It is clear through recent ICO enquiries, that not all complaints that come in from customers make it to the Data Protection team (e.g., marketing complaints and challenges over use of personal data) and additional processes and training need to be put in place by Nov 2019 to ensure that all possible 'entry/capture' points are aware of Post Office's responsibilities.

What other key funded projects are required to deliver compliance to UK DPA 18?

20. The following projects are underway, which will support Post Office's compliance with UK DPA 18:

21. Records retention; it is critical to UK DPA 18 compliance that the project continues to establish retention schedules and system and process owners implement the required deletion procedures.

22. The Joiners, Movers, Leavers (JML) project; this is a key project that is ensuring that only people who need access to personal data in order to do their job, have access. Some higher risk systems are moving to single sign on and others to enhanced manual access controls. The project will also recommend some lower risk systems that should implement stronger access controls. The project will close mid-July.

Conclusion

23. The overall compliance summary is that there has been significant improvement in Post Office's data protection processes, controls and culture. It is the opinion of the Data Protection team that Post Offices overall Compliance standing is within Risk Appetite for compliance with Legal and Regulatory obligations for all our Operational Processes. The completion of the remediation exercises highlighted in this paper will reduce the level of risk exposure and back within risk appetite for the administrative controls applied. (See the Annex below for high level information on Maturity Level of UK DPA18 compliance within Post Office.)

24. To further enhance and maintain compliance, the remediation work identified in this paper needs to be completed. This will help ensure Post Office is within its Risk Appetite for compliance with its legal and regulatory obligations and with internal Policies and Procedures.

POL00423568

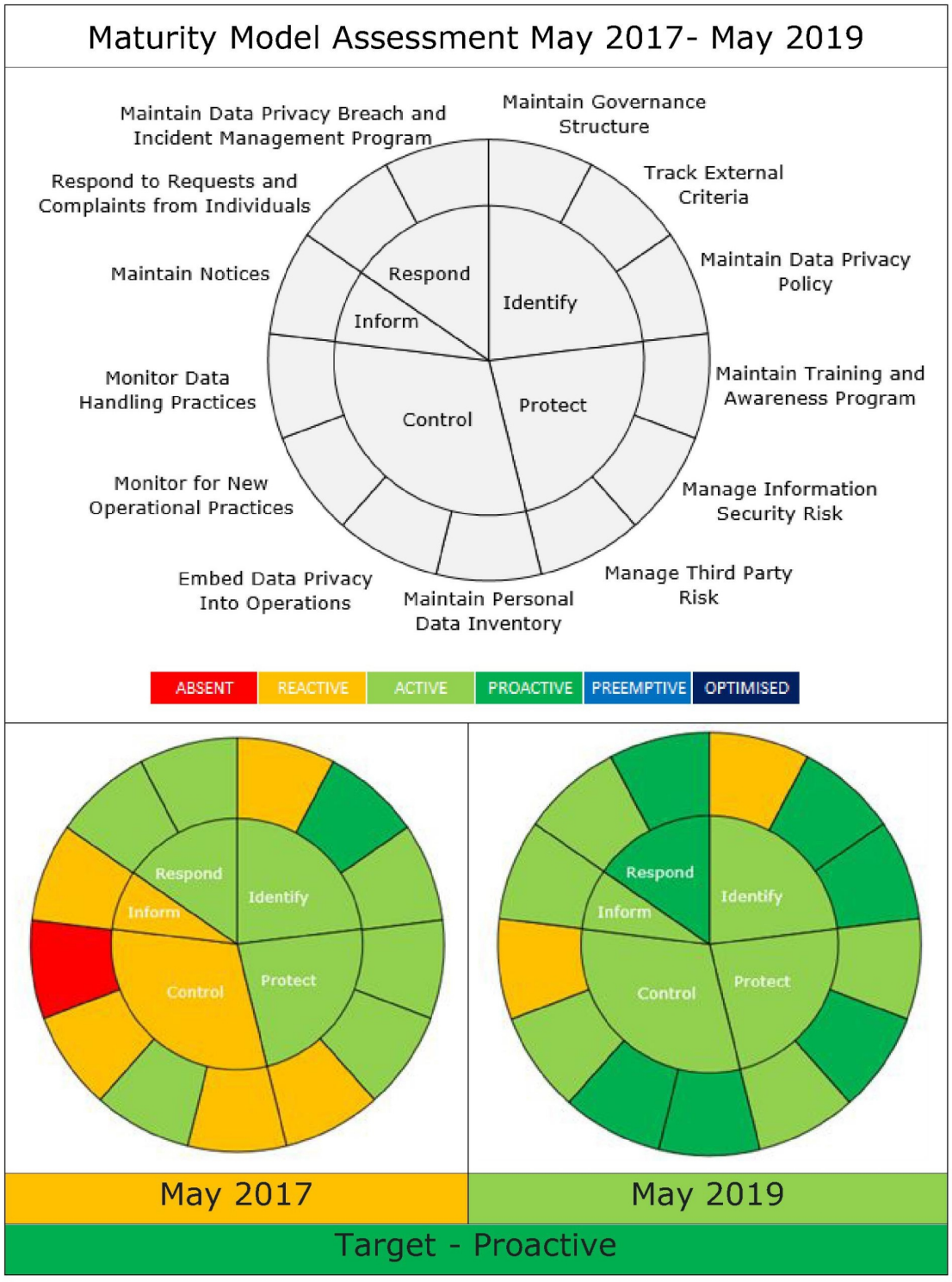
Appendix

What is the basis of this Analysis of Compliance?

1. The Post Office Data Protection Framework has been defined and is based upon the Nymity[3] Accountability model which is recognised as industry good practice. All relevant Articles of the GDPR are mapped to Privacy Management categories and activities, which in turn have been mapped to the new draft NIST (National Institute of Standards and Technology) Privacy 'functions'. It is proposed that progress will be monitored on a regular basis within a new Privacy Forum. A Privacy Dashboard is being developed, by the end of June, to track key management information and output measures such as incidents, complaints, requests and training completions etc.
2. The following diagram shows the 13 categories of the Privacy Framework around the outer wheel, mapped to the 5 NIST 'functions'. The segments are colour coded according to the maturity as per the key. Full definitions of each level are in the Appendix. The levels have been judged by the Data Protection team with input from relevant areas (e.g. IT Security).

[3] The Nymity Privacy Management Accountability Framework™ is the de facto industry standard framework for privacy management, and contains over 130 privacy management activities organised into 13 categories.

POL00423568



10

POL00423568

How was 'Proactive' determined to be the desired level of the Maturity Model and how does this fit with Risk Appetite?

3. 'Proactive' is defined as having a well-documented approach, consistently applied; having activities occur on a regular, planned basis with failures identified and rectified. A balance has been applied that provides for a robust, defendable position that protects Post Office's personal data while not overburdening the organisation.

4. Our 'Protecting Personal Data Policy' describes the Post Office as having a:

   Tolerant risk appetite for

   - Legal and Regulatory risk in those limited circumstances where there are significant conflicting imperatives between conformance and commercial practicality

   Adverse risk appetite for

   - litigation in relation to high profile cases/issues
   - not complying with law and regulations or deviation from business conduct standards
   - data loss/leakage that can lead to customer, commercial or reputational damage
   - inaccurate and unreliable processing of data

   A maturity level of 'Proactive' has been judged to sit within risk appetite.

How does the model work?

5. Each category contains a number of activities that range from 'essential for compliance' and mapped to a GDPR Article to 'enhancing' and good practice. Each activity has equal weighting within a category.

6. It is proposed that the Data Protection Team will re-evaluate the maturity score every quarter, and present at the Privacy Forum and maintain a database of evidence of controls.

10

Definition of Maturity Levels

Maturity Levels		
Score	Level	Definition
0	ABSENT	Absence or only partially present.
1	REACTIVE	Inconsistent approach; Ad-hoc, undocumented procedures; Few records kept.
2	ACTIVE	Formally resourced; Objectives are defined; Procedures defined, but are applied inconsistently.
3	PROACTIVE	Well documented approach, consistently applied; Activities occur on a regular, planned basis; Failures are identified and rectified.
4	PREEMPTIVE	Consistent and robust application; Activities are increasingly automated; Processes and tools are integrated.
5	OPTIMISED	Processes are well managed and governed by leadership; Improvements are actively sought; Monitoring captures metric to measure performance.

POL00423568

Post Office Insurance Renewal – Process Update

Author: Mark Dixon Sponsor: Micheal Passmore Meeting date: 4 July 2019

Executive Summary

Context

The business has a series of insurance policies due for renewal on IRRELEVANT A summary of the insurance programme in place at renewal in 2018 is set out in Appendix 1 (separate attachment) together with the insurance premiums paid in Appendix 2 (below, page 5 of 7). This paper provides a brief outline of the changes in approach that we are making for the 2019 renewal and sets out a summary of key milestones in the renewal process. Risk Review and Analysis is presented in Appendix 3 (separate attachment).

Question addressed in this report

How does the renewal process for 2019 differ to previous years?
What is the renewal process for 2019?

Conclusion

We believe that the change in approach adopted for the 2019 renewal will allow us to ensure we have appropriate coverage in place, with appropriate deductibles, while optimising cost and following an OJEU compliant procurement process.

11

Input Sought

The RCC members are asked to note the update on the 2019 renewal process

POL00423568

The Report

How does the renewal process for 2019 differ to previous years?

1. Our primary focus has been on delivering an insurance programme at a reasonable cost to the business. This has been achieved. IRRELEVANT

IRRELEVANT

2. POL seeks to manage the IRRELEVANT

IRRELEVANT

3. POL takes advice from its broker, Lockton, when deciding the level of these deductibles. For the 2019 renewal Lockton IRRELEVANT

IRRELEVANT

4. In order to ensure that the coverage POL has in place is appropriate we have worked with Lockton to perform a detailed risk review to identify potential gaps. Lockton have used the POL risk register as the basis for this review. The review is attached as Attachment 3. The output from this review is now being used to tailor the quotes that we requesting from insurers and therefore will enable us to make various decisions around the coverage in place.

11

5. In particular, IRRELEVANT has been identified as an area where we need to take a look IRRELEVANT This is being addressed with a small project team comprising David Mann, Tim Armit and Mark Dixon.

6. For the 2019 renewals we will follow an OJEU-compliant procurement process. The process starts with an invitation to tender that will be issued on IRRELEVANT In order to be able to comply with the process timetable we will seek approval for the renewal at the ARC meeting on IRRELEVANT

POL00423568

What is the renewal process for 2019?

7. The 2019 renewal date is **IRRELEVANT**

8. Key milestones in the 2019 renewal process are shown below:

Description	Date	Comments / Additional Notes
JULY RCC MEETING	■ 4 July	- *Papers due by 26 June* -
Issue Invitation to Tender	■ 9 July	- -
JULY ARC MEETING	■ 29 July	- *Papers due by 23 July* -
Deadline for Tender Submissions	■ 19 Aug	- -
Scoring of Submissions and Finalisation of Programme	■ 20 Aug to 13 Sep	- -
SEPTEMBER RCC MEETING	■ 3 Sept	- *Paper submissions due by 23 August* -
SEPTEMBER ARC MEETING	■ 23 Sept	- *Paper submissions due by 13 September* -
Final Decisions Required on Insurance Programme (Insurers, Structure, Terms, etc.)	■ 11 Oct	- -
Notifications Sent to Insurers	■ 11 Oct	- *There is a minimum 10-day period after insurers are notified before final contracts can be awarded.* -
Insurance Contracts Awarded	■ 23 Oct	- -
CONTRACT COMMENCEMENT	■ 1 Nov	- -

11

9. We will provide a brief update to the RCC and ARC in July and then seek approval from the September ARC. Given the deadline for tender submissions it will not be possible to provide an update to the September RCC. We will, however, meet with Al Cameron and Rob Houghton once we have quotes back from insurers and prior to submitting papers to the September ARC in order to finalise decisions around coverage.

POL00423568

Appendix 1: Summary of Insurance Programme at 2018 Renewal

Appendix 2: Insurance Premiums at 2018 Renewal

Appendix 3: Risk Review and GAP Analysis

POL00423568

Appendix 1: Summary of Insurance Programme at 2018 Renewal

See separate attachment

POL00423568

Appendix 2: Insurance Premiums at 2018 Renewal

Policy	2018/19 Premium
Crime	IRRELEVANT
Motor	
Combined Liability	
PI - POL	
PI - POMS	
Cyber	
PD & BI	
D&O	
Terrorism	
PA & Travel	
Contingency	
TOTAL	

IRRELEVANT

POL00423568

Appendix 3: Risk Review and GAP Analysis

See separate attachment

POL00423568

Post Office Group - Summary of Insurances

(based on renewal at 1 November 2018)

Insurance Line	General	Deductibles / Retention	Limit of Indemnity / Sub-limits	Comments

POST OFFICE - GROUP INSURANCE COVERAGE

IRRELEVANT

POL00423568

Tab 11 Corporate Insurance Renewal

Insurance Line	General	Deductibles / Retention	Limit of Indemnity / Sub-limits	Comments

IRRELEVANT

11

POL00423568

Post Office Principal Risks vs Insurance

Principal Risks	Risk Definition	Insurable Risk	Current Insurance	Proposed Change
OPERATIONAL	IRRELEVANT			
INFORMATION SECURITY				
TECHNOLOGY				

POL00423568



Note: a number of the risks identified above by Post Office have the potential to result in liability of directors and officers for breach of duty, duty of care etc. The organisation buys D&O insurance to address this.

POL00423568

Audit, Risk and Compliance Committee Agenda

Date:	Monday 29 July 2019	Time	14.30 – 18.00 hrs	Location	1.19 Wakefield

Present	Other Attendees	
• Carla Stent (Chair) • Tom Cooper • Tim Franklin • Ken McCall	• Alisdair Cameron (Interim CEO) • Shirine Khoury-Haq (Non-Executive Director) • Tim Parker (Chairman – PO Limited) • PwC (including Ian Morrison) (External Audit Partner) • Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Jonathan Hill (Compliance Director)	• Amanda Bowe (item 3.) (Chair, ARC PO Insurance Director) • Rob Houghton (item 5.) (Group CIO) • Tony Jowett (item 5.) (Chief Information Security Officer) • Phey Rasulian (item 5.) (Programme Manager Payment Services - Retail) • Ben Cooke (item 8.) (CIO Back Office) • Mark Dixon (item 9.) (Head of Tax & Treasury) • Andy Bear (item 9.) (Insurer Account Manager, Locktons)
	• Ben Foat (General Counsel)	• Tim Armit (item 10.) (Business Continuity Manager)
	• Micheal Passmore (Finance Director)	• Tim White (item 11.) (PMO Lead)
	• David Parry (Senior Assistant Company Secretary)	
Apology:		

	Agenda Item	Action Needed	Lead	Timings
1.	**NEDs meeting with Internal Auditors**		Johann Appel	14.30 – 15.00
2.	**Welcome and Conflicts of Interest**	Noting	Chair	15.00 – 15.05
3.	**Update from Subsidiaries:** • Post Office Management Services ARC (Verbal)	Noting & Input	Amanda Bowe	15.05 – 15.10
4. 4.1 4.2 4.3	**Minutes and Matters Arising** Minutes of the Audit, Risk and Compliance meeting held on 29 May 2019 Actions List Draft Minutes of the Risk and Compliance Committee held on 4 July 2019	Approval Noting & Input Noting	Chair	15.10 – 15.15
5.	**PCI-DSS Update and Cyber Security Update**	Noting	Rob Houghton/Tony Jowett/Phey Rasulian	15.15 – 15.30
6.	**Annual Report and Accounts** Focus on GLO disclosure	Noting & Input	Micheal Passmore / PwC	15.30 – 16.00
7.	**Consolidated Report from Internal Audit, Compliance and Risk Department**	Noting & Input		16.00 – 16.45
7.1	Risk Report		Jenny Ellwood	16.00 – 16.15
7.2	Compliance Report		Jonathan Hill	16.15 – 16.30
7.3	Internal Audit Report		Johann Appel	16.30 – 16.45
8.	**Back Office Transformation**	Noting & Input	Ben Cooke	16.45 – 17.00

12

DRAFT

POL00423568

Audit, Risk and Compliance Committee Agenda

9.	**Corporate Insurance Renewal**	Noting & Input	Mark Dixon/Andy Bear	17.00 – 17.15
10.	**Business Continuity Update**	Noting & Input	Tim Armit	17.15 – 17.25
11.	**Proposals for Deep-Dives including update presentation from Tim White, PMO Lead on Change**	Noting & Input	Johann Appel/Jenny Ellwood/Jonathan Hill/Tim White	17.25 – 17.45
12.	**GDPR Update**	Noting	Jonathan Hill	17.45 – 17.55
13.	**Any other Business** Note: Date of next meeting 23 September 2019, 08.30 – 10.30 hrs	Noting	Chair	17.55 – 18.00

DRAFT