POL00423508

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) • Tim Parker (Chairman – PO Limited) • Ben Foat (General Counsel) • Andrew Paynter, PwC (External Audit Partner) • Stewart Light, PwC - by telephone (External Audit, Director) • Lucy Mason, PwC (External Audit, Senior Manager) • Johann Appel (Head of Internal Audit) • Jenny Ellwood (Risk Director) • Jonathan Hill (Compliance Director) • Kathryn Sherratt (Interim CFO)	• Micheal Passmore (Finance Director) • David Parry (Senior Assistant Company Secretary) • Rob Houghton (item 5.) (Chief Operating Officer) • Mark Fabes (item 5.) (Interim Group CIO) • Phey Rasulian (item 5.) (Programme Manager Payment Services, Retail) • Tony Jowett (item 5.) (Chief Information Security Officer) • Ben Cooke (items 8, 9.) (CIO Back Office) • Tim Armit (item 10.) (Business Continuity Manager) • Tim White (item 11.) (PMO Lead)
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	Tim Franklin	15.05 – 15.10
4. 4.1 4.2 4.3 4.4	**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 Disaster Recovery testing August Bank Holiday weekend	Approval Noting & Input Noting Noting	Chair	15.10 – 15.15
5.	**PCI-DSS Update and Cyber Security Update** • PCI DSS • Cyber Security includes review of recent data breaches from BA, Marriott and Facebook	Noting	Rob Houghton Phey Rasulian/Mark Fabes Tony Jowett	15.15 – 15.30

POL00423508

Audit, Risk and Compliance Committee Agenda

6.	**Annual Report and Accounts** – focus on GLO & Starling disclosures	Noting & Input	Ben Foat/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.	**Transtrack, Back Office Transformation**	Noting & Input	Ben Cooke	16.45 – 17.00
9.	**Belfast Data Centre Disaster Recovery**	Noting & Input	Ben Cooke	17.00 – 17.15
10.	**Business Continuity Update**	Noting & Input	Tim Armit	17.15 – 17.30
11.	**Deep-Dive Presentation – Update on Change** includes proposals for future deep-dives	Noting & Input	Tim White Johann Appel/ Jenny Wood Jonathan Hill	17.30 – 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

POL00423508

Risk Management and Compliance Report

Author: Ian Holloway, POI Director Risk and Compliance

Meeting date: 29 July 2019

Executive Summary

Context

This paper provides a concise summary for the POL ARC of matters considered within the POI ARC meeting on the 18 July 2019.

Questions this paper addresses

1. What are the key points considered within the Risk and Compliance meeting which the Board should be aware of?

Input Sought

The report is provided for information and discussion.

The Report

1. What are the key points considered within the Risk and Compliance meeting which the POL Board should be aware of?

- **Year-end statutory accounts** - the ARC received the final report from the external auditors. The 2018/19 accounts are being finalised pending completion of a small number of outstanding audit deliverables but nothing of concern had been flagged.

  It is expected that the Board will review the finalised year-end accounts for approval by 31 July 2019. The POI CFO had provided the directors with an overview of the assurances they could take in being satisfied it was appropriate to recommend signing the management representation letter.

  Following consideration of the audit report, the ARC will continue to closely monitor the assessment of goodwill impairment throughout 2019/20, noting it was sensitive to any changes affecting growth assumptions within the five year plan. Costs were volatile year on year due to the inclusion of the larger spend on capex, aggregator costs, people and marketing to support the expected growth in home and life business. The application of the new

POL00423508

accounting revenue standard IFRS15 (Revenue from Contracts with Customers), has been worked through. It introduced an element of volatility into future years' accounting which would be closely monitored. Reflecting on lessons learned, the ARC noted that going forwards there would now be closer alignment between Group and POI Finance teams to ensure that there was a greater shared understanding of each other's work. Internal governance had been strengthened to ensure POI would be included within the scope of Group Finance work assessing any new accounting standards and legislative changes.

- **External Audit Findings** - The POI ARC wish to bring the internal control recommendations relating to access to Post Office systems (including Horizon) to the attention of the POL ARC. In essence it is not clear that there are effective controls to ensure that leaving staff are promptly removed from the system. Similar matters had been highlighted by auditors in previous years and the POI ARC wished to understand (i) the barriers to resolution (ii) the dynamics of the risk POI and POL were being asked to accept until the matters were resolved. Systems access controls are important to POI in ensuring that staff are fit and proper, and that they have been properly trained amongst other areas.

- **Reappointment of External Auditors**- The POI Board approved the reappointment of the external auditors (PwC) on the recommendation of the ARC.

- **Internal Audit progress**-There has been good progress closing IA actions due within the period. The Nemesis in-flight report had been issued and the Product Lifecycle review report would be issued in advance of the September ARC. The Nemesis review observed that significant progress has been made by POI in Change maturity by incorporating its own lessons learnt and the recommendations from previous audit reports. Recommendations were made around maintaining an appropriate level of programme controls, particularly in documenting and managing requirements; in risk and dependency management across all work streams; and in programme level activities such as documenting internal changes. Programme delivery was manual and reliant on individual capabilities rather than a defined process aided by proven programme management tools. Management was in the processes of deploying tools and had since addressed the issue.

  A risk remained in regards to reliance of individuals although this was currently being managed through tight oversight by the programme leadership. Planning more generally is underway on succession planning and on ensuring more effective transition of contractor skills.

POL00423508

- **Financial Crime** – The ARC received updates from Sally Smith on Whistleblowing in addition to a report on AML, ABC and CTF risks. The ARC recommended that:
    - the POL ARC receive an overview of the annual POI MRLO report.
    - going forwards, the POI ExCo receive regular gifts and hospitality reporting in addition to the POI ARC's continued oversight.
    - infrastructure to support whistleblowing be extended to third parties.

- **Third party oversight work**: The ARC was pleased with the third party control framework presented. Following feedback provided at the meeting, oversight measures would include whistleblowing, culture and ethics in addition to those areas set out in the report.

- **Complaints deep dive**: The July meeting focused on Protection and getting behind the data, identifying any emerging trends and examining the effectiveness of policies / processes in place. Deep dives on complaints by product area will be a regular feature of future meetings.

- **Oversight of the AR and mystery shopping results** – Following completion of the improved control framework the ARC is satisfied that it has taken the necessary steps to systematically bring the AR risk within appetite and there had been an overall improvement in this regard. However, there remain issues with the quality of branch sales as evidenced by disappointing mystery shopping results in the period (c23% of shops being graded as "red). There will be a concentrated effort to improve the quality of branch sales and the ARC will review performance in September, allowing time for the integration of a new network sales model.

- **ERV and the Transition from TIF-** No further business is now being placed with TIF from 1 July 2019. This follows the successful establishment of ERV as our new joint underwriter alongside Collinson. Issues have been experienced in gaining MI from TIF and at the time of the ARC TIF were challenging our ability to terminate the contract. Subsequent to the ARC, agreement on termination has been achieved and a meeting is scheduled to discuss an orderly run-off of the remaining TIF based policies between now and 30 June 2020. Management will continue to be vigilant in ensuring good customer outcomes for our customers.

- **Brexit is an increasingly prominent risk** – a 'hard' exit on 31 October is now a significant risk. POI has previously highlighted the potential impact on travel and motor business, as well as the potential for a more general financial impact, should Brexit lead to a recession. Existing risk mitigation plans are being refreshed and will be presented to the September ARC. The need to ensure that a clear Brexit position with TIF was noted in the course of the ARC.

POL00423508

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

3.1

MINUTES OF A MEETING OF THE AUDIT AND RISK COMMITTEE OF POST OFFICE LIMITED HELD ON WEDNESDAY 29 MAY 2019 AT 20 FINSBURY STREET, LONDON EC2Y 9AQ AT 14.00 PM

Present:	Carla Stent	Chair **(CS)**
	Tim Franklin	Non-Executive Director **(TF)**
	Tom Cooper	Non-Executive Director **(TC)**
	Ken McCall	Senior Independent Director **(KM)**
In Attendance:	Alisdair Cameron	Interim CEO **(AC)**
	Ben Foat	General Counsel **(BF)**
	Andrew Paynter	Group Audit Partner, PwC **(AP)** (by telephone)
	Stewart Light	Systems and Controls Director, PwC (by telephone) **(SL)**
	Lucy Mason	Group Audit Senior Manager, PwC **(LM)**
	Chris Neale	Assurance, Director, PwC **(CN)**
	Johann Appel	Head of Internal Audit **(JA)**
	Jonathan Hill	Compliance Director **(JH)**
	Deana Hurley	Senior Manager, Assurance (deputising for Jenny Ellwood) **(DH)**
	Tom Lee	Head of Finance, Financial Accounting and Controls (deputising for Micheal Passmore) **(TL)**
	Veronica Branton	Head of Secretariat **(VB)**
	David Parry	Senior Assistant Company Secretary **(DP)**
	Amanda Bowe	Chair, ARC PO Insurance **(AB)** (item 2.) (by telephone)
	Rob Houghton	Group Chief Information Officer (item 5.)
	Tony Jowett	Chief Information Security Officer (item 5.)
	Elizabeth Robson	Change and IT Director **(ER)** (item 5.)

Action

1. Welcome and Conflicts of Interest

CS welcomed everybody to the meeting and noted it had been re-arranged due to AC attending a Select Committee meeting on 21 May.

The Directors declared that they had no new conflicts of interest in the matters to be considered at the meeting in accordance with the requirements of section 177 of the Companies Act 2006 and the Company's Articles of Association.

2. Update from Subsidiaries

Amanda Bowe (AB) provided an overview by telephone of the key issues discussed at the recent Post Office Insurance (POI) ARC meeting of 14 May 2019, and noted the positive Board risk workshop held on the same day.

Risk workshop
Key points emerging from the workshop included the importance of due diligence to reduce information security leaks; the oversight of financial risks particularly at the second line of defence required consideration; and POI's risk appetite needed enhancing.

POI ARC
The following key issues were discussed at the recent POI ARC meeting:

- A cultural review would be completed to ensure that the business plan and good customer outcomes were achieved. The risks to POI's strategy would also be reviewed.

DRAFT

POL00423508

- The FCA had recently published its 2019/2020 business plan and was more clearly defined than previous years. Focus was on governance, culture, and specifically for general insurance, on product value, pricing and market access.
- POI was developing its appetite for reputational risks but recognised that momentum required maintaining.
- Mystery shopping results in March and April had significantly improved.
- Good progress had been made in the transition of the travel business underwriter from TIF to ERV.
- Two security breaches had been reported to the regulator, but no further action would be taken by the regulator, and no further breaches had been reported. AB noted the importance of handling customer information with care.
- The Committee had noted the good progress to bring the Appointed Representative status within risk appetite by June 2019.

The Committee sought and received confirmation that reasonable progress had been made with POI's financial statements for the year 2018/2019.

AB left the meeting.

3. Minutes and Matters Arising

3.1 The minutes of the meeting of the Audit and Risk Committee held on 25th March 2019 were **APPROVED** and **AUTHORISED** for signature by the Chairman.

3.2 Progress with the completion of actions as shown on the action log was **NOTED**. The Chair noted that a number of actions due at this meeting would now be discussed in July.

3.3 The draft minutes of the Risk and Compliance Committee held on 9 May 2019 were **NOTED**.

4. Annual Report and Accounts 2018/2019 (ARA)

4.1 CS commented that the Board had delegated authority to the Chairman and Interim CEO to sign off the annual report and accounts for 2018/2019 and that good progress had been made to date with further work required before sign off.

TL remarked that the ARA was in a good position overall and that comments received from UGKI and POL directors had been reviewed and responded to. The finance team was comfortable with the numbers presented but noted these were subject to change depending upon PwC's audit findings and further internal review, although he did not expect these changes to be significant.

To date, neither PwC nor management had identified any significant issues that would deter sign off.

4.2 **Risk Management Section ARA 2018/2019**

DH ran through the risk section of the ARA which had been discussed at the recent Risk and Compliance Committee meeting (9 May).

Two new top risks of Health and Safety and the Group Litigation had been identified for inclusion into the ARA.

The Committee questioned the inclusion of Health and Safety as a top risk considering the year on year improved standards at POL. DH responded that while this was the case, it had been a Top Risk within the Group Risk profile for over the past couple of years, POL operates a sizeable fleet and increased levels of cash made some colleagues more vulnerable to crimes against the Post Office and fact that the directors of POL were

DRAFT

POL00423508

personally liable for health and safety had prompted the view that it should be included. The Committee agreed health and safety should be included as a top risk.

Group Litigation had been included due to the increased likelihood that legal findings and court orders would have an adverse impact on financial performance and/or reputation, moving from 'unlikely' to 'possible'.

Regarding the Technology, Business Interruption and Cyber risk, KM believed the movement should remain flat. A number of mitigating actions had been introduced but POL was some way off being best in class.

Regarding the Regulatory Environment, the Committee agreed the movement should remain flat.

The Committee noted the risks presented and agreed the revised rating indicators.

4.4 **Group Litigation**

CN advised that the audit work on Group Litigation would be completed as late as possible due to the continued movement in the situation and the associated disclosure.

It was noted that it was difficult to provide a reliable estimate for a provision at present because the claimants had not formalised claims. Management agreed to support PwC to seek, in writing, from legal counsel, the reasons that POL was currently unable to provide a reliable estimate. BF

4.5 [redacted]

4.6 **Fraud**

CN noted that the auditors had to consider the possibility of fraud in relation to management override of controls and the risk of fraud in revenue recognition. Although work was on-going, no issues had been identified to date.

4.7 **Other**

Gamma - POL currently holds deferred income of IRRELEVANT which is released to revenue at IRRELEVANT per year until 2022/23. This relates to a contractual agreement with the Bank of Ireland from 2008 where IRRELEVANT IRRELEVANT

The auditors are reviewing the contractual obligations to confirm the accounting treatment. Both AC and JH believed that both parties intended for there to be an ongoing obligation.

4.8 **IT Access**

SL advised that a number of Global Users (primarily audit and admin staff who have since left the organisation) had been found to have still access to the Horizon system, the main system used by POL branches.

BF remarked that this had been discussed internally and that POL's external legal advisers had advocated its disclosure at Group litigation. He noted that of the 32 former agents who had had access, none had accessed the system since leaving POL.

POL00423508

The Committee noted that the maintenance of joiners and leavers was an ongoing issue that had been raised at ARC on numerous occasions, and sought assurance that the executive would resolve the outstanding control weaknesses.

AC undertook that accountability for resolution would be held by the Group Executive, which would report back to the ARC on steps taken to implement and test the necessary controls. **AC**

4.9 CS thanked the audit team and the finance team for the work completed to date. Updated documentation would be presented to the Committee at the end of June to early July. **Executive /PwC**

4.10 **External Auditor Re-Appointment for 2019/20**

The appointment of PricewaterhouseCoopers LLP as external auditors for the year 2019/20 was **APPROVED**.

5. PCI-DSS Update and Cyber Security Update

5.1 Rob Houghton, Elizabeth Robson and Tony Jowett were welcomed to the meeting. Tony Jowett provided a brief career background to date following his recent appointment as Chief Information Security Officer at POL. The Committee noted he lead the Deloitte audit team on cyber security at POL.

5.2 **PCI-DSS Update**

LR provided a current update.

The data audit had now been completed and any outstanding actions would be completed by the end of May. Low or no instances of PCI related data had been found; users had been educated to prevent further occurrences.

The project to replace the pin-pad devices in branches (that provide access to the estate) was well underway with completion scheduled for March 2020. This would also include a software update.

The alternative solutions to processing banking data (avoiding the routing of data via Horizon) was found to be technically feasible and work was now in the detailed design stage with Ingencio, Vocalink and Fujitsu.

KM sought confirmation on how long the detailed design stage would take to complete. RH believed this stage could be completed by the third quarter of 2020 (calendar), but that greater pressure was required for Ingencio to prioritise the work. Current estimates for delivery were not felt to be acceptable by the Committee.

TF requested a firm timeline setting out the deliverables, associated risks and costs.

It was **AGREED** that KM and CS would assist with any calls to Ingencio (Paris branch) should they be required and requested RH provide an update within the next ten days. RH

LR left the meeting.

5.3 **Cyber Security**

RH provided an update on Cyber Security.

The team had made progress with POL's security strategy focusing on improving the reach and capability of the Security Operations Centre; improving data security; and improving governance around 3rd party cyber security.

DRAFT

POL00423508

TF requested that the 3rd party governance be reviewed for Post Office Management Limited. CS noted that RSA Archer needed to be fully implemented and was key to our management of 3rd party governance. RH

KM sought clarification of the data breach in February where POL user data was placed on the dark web for sale. RH assured the Committee that this issue had been rectified and that a communication to POL staff about the danger of registering work email addresses on third party applications/websites had been circulated.

It was agreed the at the Committee would keep this as a recurring agenda item.

Payzone

Mitigating actions had been implemented to rectify the issues raised following penetration testing at Payzone. The security team would also being visiting Payzone in June.

CS thanked the team for their work.

RH and TJ left the meeting.

6. Consolidated Internal Audit, Compliance and Risk Report

6.1 The Committee noted this was the first time a consolidated report for Internal Audit, Compliance and Risk had been presented. Additional material was available in the reading room.

6.2 **Internal Audit**

JA presented the Internal Audit report.

He advised that the programme was almost complete with 24 of the 26 planned audits being delivered on plan. Seven reviews had been completed since the March ARC meeting.

Completion of the Contract Management internal audit report had been impeded by the lack of a clear ownership and IT Control Framework internal audit report had also been delayed. It was noted the contract management internal audit report had been outstanding since January 2019.

The Committee registered their disappointment at the failure to identify a clear owner for contract management and it was agreed that AC would resolve this. Additionally, KM reiterated that audit reports should not be held back because of failure to receive management input. Audit reports should be presented to ARC within one quarter of the planned completion date, whether management comments had been included or not and should be flagged as 'red' where no management commentary had been provided. AC

It was **AGREED** the outstanding Internal Audit reports would be circulated to the Committee. JA

TC sought assurance that POL met the compliance requirements for the network reporting contracts. AC assured the Committee that the network team owned these contracts and that they were managed compliantly. The full report on the management of these contracts would be sent to TC. JA/AC

CS sought and received confirmation from JA that he was satisfied with the work completed to date and with the working relationship work with Deloitte. JA reported that Deloitte Partners were interested in, and reviewed the internal audit reports and he was satisfied a good quality assurance programme had been established.

DRAFT

POL00423508

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

6.3 **Compliance**

JH presented the Compliance report and highlighted the following key points.

Text relay

Ofcom had issued a formal information request and work with Fujitsu was ongoing to meet Ofcom's requests. He noted that Ofcom wished understand the position from 2003/04 but noted that POL might not hold all of this information. JH noted that Ofcom had been positive about the corrective actions implemented to date and POL's willingness to settle early.

End of contract negotiations

Ofcom had "invited" all telecoms companies to sign up to a voluntary charter setting out six principles of fairness to customers. POL planned to sign up to this charter. Good progress had been made with POL's commitment to look after vulnerable clients.

KM raised the appropriateness of IRRELEVANT IRRELEVANT

AC responded that he was due to meet the new CEO of IRRELEVANT shortly, and that POL had no plans in place to reconsider them as a franchise owner. From POL's point of view, IRRELEVANT was a strong retailer and as the IRRELEVANT IRRELEVANT had considerable high street presence, generally providing a good service to Post Office customers. POL would however continue to encourage IRRELEVANT to improve customer service standards and had incentivised this through the Project Edgware franchising arrangements.

The Committee requested that conversations on customer service standards be held with IRRELEVANT and that an appropriate audit trail of these conversations be recorded. To do: Executive

Fit and Proper

HMRC had agreed to extend the deadline for MI collection to September 2019 from June. Considerable progress has been made in data collection and the team was still aiming to have the work completed by June.

Branch Registration fees

HMRC had increased their fees from £130 per annum to £300 per annum from 1 May 2019.

6.4 **Risk**

DH presented the Risk report and highlighted the following key points.

Since the last meeting, PCI Compliance and Group Litigation remained as 'red' risks, and a number of emerging risks including changes in work force, Brexit and the loyalty super complaint had also been identified. No major changes had been made to the Heatmap.

Regarding PCI, and as noted above, whilst a definitive timeframe for completion had not been determined, work was underway to identify a more aggressive timeframe than the proposed November 2020 timeframe provided.

The second High Court trial relating to the Horizon system resumed on 4 June 2019 and was due to run until 1 July 2019. Assistance has been requested from Deloitte to prepare for all potential judgement scenarios.

There had been a number of changes in key personnel since the last ARC meeting and further organisational design changes were planned which had led to the identification of

POL00423508

an emerging people risk. The Committee discussed this and it was agreed that this was not a significant increase in the risk, given historic turnover comparisons. DH agreed to reflect a revised assessment. DH

Uncertainty surrounding Brexit and political certainty remained, with any ultimate implications for POL remaining unknown at this point.

A watching brief on the loyalty super complaint remained in place and the outcome was still awaited. Ofcom had unveiled new rules requiring broadband, phone and TV providers to inform customers of their best deals at the end of their existing contracts.

Following the results of planned penetration testing of Payzone devices and front-end network, it was IRRELEVANT. Work is underway to remediate this and is expected to be completed by October and a wider risk identification workshop will be held with Payzone to align management risks in line with the POL framework. A Risk Business Partner has also been allocated to support this work and future engagement.

The future of the Post Office Card Account (POCa) was raised. POCa enabled the government to pay benefits to people without bank accounts. The potential difficulties for those individuals without access to such an arrangement was noted. AC remarked that a conversation with Amber Rudd was required and that the replacement for the POCa arrangement could be an opportunity to solve a wider financial access problem.

Regarding GDPR, DH was requested to provide a current update at the next meeting.

CS requested that the learnings from the Change risk be taken on board to ensure future projects incorporated these learnings. CS noted that she had requested an overview of the function and the governance structures by Tim White at the next ARC. Tim White

7. AOB

There being no further business, the meeting closed.

DRAFT

Not Cast

.....

Chairman Date

Actions from meeting

Minute	Action	Lead	Due Date
4.4	**ARA 2018/2019** – Group Litigation, provide support to PwC to seek in writing, from legal counsel, the reasons that POL is currently unable to provide a reliable estimate for disclosure..	BF	ASAP
4.8	**ARA 2018/2019** – IT access, report back on steps taken to implement and test necessary controls regarding user access to Horizon by former agents.	AC	July
4.9	**ARA 2018/2019** – updated documentation to be provided by the end of June/beginning of July.	Executive/PwC	End June/early July
5.2	**PCI-DSS** – To provide an update from conversations with Ingencio (Paris branch) regarding Ingencio re-prioritising POL work.	RH	Early June

POL00423508

POST OFFICE LIMITED AUDIT AND RISK COMMITTEE MEETING
Strictly Confidential

5.3	**Cyber Security** – Review 3rd party governance for Post Office Management Limited.	RH	July
6.2	**Internal Audit** – Contracts Management owner to be identified and allocated.	AC	July
6.2	**Internal Audit** – to circulate the outstanding Internal Audit reports.	JA	ASAP
6.2	**Internal Audit** – Network Reporting contract, management report to be sent to Tom Cooper.	JA/AC	ASAP
6.4	**GDPR** – update to be provided.	JH	July
6.4	**Change Risk** – overview of function and governance structures to be presented at next ARC meeting.	Tim White	July

DRAFT

POL00423508

Voting Results for Minutes of the Audit, Risk & Compliance Committee meeting held on 29 May 2019

The signature vote is still in progress. 1 votes are required to pass the vote, of which 0 must be independent.

Vote Response	Count (%)
For	0 (0%)
Against	0 (0%)
Abstained	0 (0%)
Not Cast	1 (100%)

Voter Status

Name	Vote	Voted On
Stent, Carla	Not Voted	

POL00423508

REF.	ACTION	ACTION OWNER	DUE DATE	STATUS	OPEN / CLOSED
30 October 2018					
11. Insurance Policies	Review the risks covered by the suite of Insurance policies.	**Jenny Ellwood**	~~May 2019~~ ~~July 2019~~ September 2019	~~Update to be given at the May ARC meeting. Following discussion with the Chair, an update will be provided in the July ARC meeting.~~ An update will be provided at the September ARC meeting.	Open
29 January 2019					
2. (b)	ARC to review the quality of sales of financial services products in the branch network in more depth.	**Jonathan Hill**	~~May 2019~~ July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open
6. Money Laundering Reporting Officer (MLRO) Annual Report					
6. (a)	To provide regular updates on the complete fit and proper data to HMRC.	**Nick Boden/ Sally Smith**	Ongoing	**Ongoing until project close.** Item included on ARC agenda.	Open
7. Security Strategy					
7. (a)	To provide quarterly reports to the ARC showing how we were performing against the metrics agreed to implement the Security Strategy once the deep dive with Deloitte had taken place.	**Rob Houghton / Mick Mitchell**	May 2019	**Ongoing.** Item included on ARC forward agenda.	Open
9. Audit Strategy Memorandum	To consider a deep dive on Successfactors given the cost of the system and its limited functionality.	**Exec**	~~May 2019~~ July 2019	Proposals for deep dives and the sequencing of these will be brought to the May ARC meeting. Proposals will now be brought to the July ARC meeting.	Open
25 March 2019					
4. Compliance Report -					
4. Telco	Consider whether we should write off ETCs where a complaint is received. This could save time and resource costs.	**Jonathan Hill/Meredith Sharples**	May 2019	Customers joining enter a 12, 18 or 24 month contract which protects our commercial interests and their rights to service at a fixed cost, if either party break this contract then a penalty applies. This penalty works for the customer and for POL e.g. if we raise the prices then customers can leave early without charge or if a customer chooses to leave early then we are entitled to charge a fee for Early Termination Charge (ETC) Any customers who complain follow a standard process by which their grievance is evaluated on a case by case basis, in the case of ETCs this can sometime lead us to cancel the charge.	Recommended for closure

POL00423508

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 22.07.19

				Our focus on customer is demonstrated by Ofcom reported complaints where we are below the industry average and have reduced by 33% YoY driven by our Customer First programme. Our complaints specifically around ETCS are at record low levels and are down 23% YoY.	
5. Risk					
5. PCI Compliance	Check whether any of the additional credit card data we hold contains personal data and whether this had been covered as part of the GDPR work programme.	**Mick Mitchell/ Liz Robson/ Jonathan Hill**	May 2019	The GDPR programme looked at how we use all credit card (PCI) data across the business. PCI-related data would also be categorised as Personal Data, under GDPR. As part of the Process Mapping exercise, we have identified where this data is captured across our processes and procedures. The Data Audit addressed any PCI-related data held in systems.	Recommended for closure
5. PCI Compliance	Circulate the updated scope for PCI compliance and the plan and timeline for its delivery as soon as the plan has been agreed (18 April 2019 is the target date).	**Mick Mitchell/ Liz Robson**	May 2019	The update report was issued to ARC members on the 25th April 2019. A further update paper will be provided as pre-read for the ARC meeting on the 29th May 2019.	Recommended for closure
5. Cyber Security Report	The Information Security Committee should be accountable for the Cyber Security implementation strategy and should report back to ARC on this. The plan needed to take into account all the recommendations from the Deloitte Report and work out a priority plan.	**Jane MacLeod / Rob Houghton**	May 2019	An update is provided within the Cyber Security report.	Recommended for closure
5. Risk Appetite for Information Security	Provide an answer urgently on what the data was contained in the 140k files shared with external users.	**Mick Mitchell**	May 2019	An update is provided within the Cyber Security report.	Recommended for closure
7. Back Office Transformation	Provide an update on Back Office Transformation and the position with Transtrack.	**Executive**	May 2019	~~An update will be provided in the CEO paper to the Board in May.~~ An update will be presented at the July ARC meeting.	Recommended for closure
9. Treasury Policy	Executive consider whether it would be appropriate to have two hedging arrangements in place for foreign exchange, one to deal with short term currency	**Executive**	May 2019	Reading materials can be found in the Reading room.	Recommended for closure

POL00423508

Post Office Limited – Audit, Risk and Compliance Committee Actions List
Updated 22.07.19

	fluctuation, the other with the longer term position.				
29 May 2019					
4.4 ARA	ARA 2018/2019 – Group Litigation, provide support to PwC to seek in writing, from legal counsel, the reasons that POL is currently unable to provide a reliable estimate for disclosure.	**BF**	ASAP	An update will be provided at the July ARC meeting.	Recommended for closure
5.2 PCI-DSS	To provide an update from conversations with Ingencio (Paris branch) regarding Ingencio re-prioritising POL work.	**RH**	Early June	A meeting was held with Ingenico who have re-prioritised POL work.	Recommended for closure
6.2 Internal Audit	**Internal Audit** – Contracts Management owner to be identified and allocated.	**AC**	July	An owner has now been allocated.	Open
6.2 Internal Audit	**Internal Audit** – to circulate the outstanding Internal Audit reports.	**JA**	ASAP	Completed.	Recommended for closure
6.2 Internal Audit	**Internal Audit** – Network Reporting contract, management report to be sent to Tom Cooper.	**JA**	ASAP	Completed.	Recommended for closure
6.4 GDPR	**GDPR** – update to be provided.	**JH**	July	An update will be provided at the July ARC meeting.	Recommended for closure
6.4 Change Risk	**Change Risk** – overview of function and governance structures to be presented at next ARC meeting.	**Tim White**	July	An update will be provided at the July ARC meeting.	Recommended for closure

POL00423508

3.3

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 4 July 2019 at 13.00 pm

Present:	Alisdair Cameron (Chair) (AC)	Interim Chief Executive Officer
	Chrysanthy Pispinis (CP) (on behalf of Owen Woodley)	Senior Strategy Manager
	Ben Foat (BF)	General Counsel
	Rob Houghton	Group Chief Information Officer
	Mo Kang	Group HR Director
	Cathy Mayor (CM) (on behalf of Debbie Smith)	Finance Director, Retail
In Attendance:	David Parry (DP)	Senior Assistant Company Secretary
	Johann Appel (JA)	Head of Internal Audit
	Jenny Ellwood (JE)	Risk Director (via telephone)
	Jonathan Hill (JH)	Compliance Director
	Mark Fabes (MF)	Interim Group CIO (items 1-3)
	Tony Jowett (TJ)	Chief Information Security Officer (item 4)
	Tim Armit (TA)	Business Continuity Manager (items 4,
	Ben Cooke (BC)	IT Director – Back Office (item 5)
	Barbara Brannon (BB)	Purchasing Director (item 7)
	James Scutt (JS)	Head of Customer Experience, Retail (item 9.3)

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**

AC opened the meeting and remarked that the pack was too large and should be halved in length. Papers should be condensed to identify the most significant risks and issues faced by the Post Office, the mitigating actions that were being completed and the timeframes for doing so.

2. Minutes and Action Lists

The minutes of the RCC meeting held 5 May were **APPROVED.** Progress on completion of actions as shown on the action log were **NOTED.**

3. PCI-DSS Update

The paper was taken as read.

RH outlined that there are two types of transactions; retail and banking. Both transactions require pinpad upgrades with the banking transaction requiring a solution that avoids PAN data being brought into the POL environment (called the "banking solution" for ease).

AC sought and received confirmation from RH that no definitive plan had been received from Ingenico regarding the banking solution. A plan for collection, shipment and firmware upgrade and in-branch device swap had been agreed, and a pilot to update the pin-pad devices was scheduled to begin at the end of August, with a full roll-out planned in September on successful completion of the pilot.

POL00423508

It was noted that the pin-pad devices could only be upgraded by trained specialists and not in-house. For the banking solution, resource to commence the design activities had been provided by Vocalink and Fujistu, Ingencio had advised that they could not provide suitable resource until late August/early September.

In order to avoid further delay, AC requested that escalation with the senior executive of Ingencio be accelerated. **RH**

The RCC discussed further the banking solution and the two opportunities to improve POL's PCI compliance status currently being explored. Firstly, to identify whether there were any alternative providers (such as Global Payments) who could process banking transactions reducing POL's reliance on Ingencio, and secondly, to explore whether banking transactions could be excluded from PCI-DSS regulation. RH commented that POL's legal team had engaged with CMS (Solicitors) and the Payment Service Regulator (PSR) to confirm this position, and that feedback was expected by the end of July/early August.

The RCC noted that whilst banks comply with PCI, they are not certified/subject to PCI compliance, whereas merchants are. Additionally, PCI was recognised as a good industry standard to meet, and POL would strive to meet this as business as usual.

The recent Data Audit had now been completed and no further instances of PCI related data had been identified. A full report was expected by the end of July.

AC requested that a condensed paper of two sides be prepared ahead of the next ARC meeting (29 July) clearly communicating the current position.

MF left the meeting.

4. Security Strategy

4.1 The paper was taken as read.

TJ and TA entered the meeting.

TJ explained that the purpose of the paper was to provide an update of the current position. In line with best practice and to meet the recommendations of the Deloitte Review, the Cyber Security Team had now been expanded to cover IT Security and Business Continuity Management. Prioritisation had been given to meetings with key third parties to understand and align on security provision.

AC questioned when POL's position could be considered 'Good'. TJ responded that the process of designing 'Good' was in train, and that seven of the ten key recommendations from the Deloitte Review had now been met. Additionally, a number of initiatives throughout the year had identified POL's 'Crown Jewels' i.e. the business critical data/systems, its location and the controls in place to protect this. GDPR was not considered part of the 'Crown Jewels' as GDPR relates to personal data rather than business critical data.

CP questioned whether agent related data (such as agent pay) was considered part of the crown jewels. BF believed this should be treated as part of the 'Crown Jewels' and noted that the Secretariat department had good governance controls in place regarding the storage of business critical data such as financial data, litigation material and business reports. A cultural piece was required across POL to ensure that business critical data was treated with a greater sense of security.

He suggested that as a starting point, the team should review the document retention programme listing all corporate documents, owners and the retention period.

POL00423508

AC requested that the term 'Crown Jewel' be more clearly defined. Regarding third party data, this should clearly identify the type of data held/stored, the audit rights and when they can be exercised.

Further, it would be useful for the RCC to see a report that identified: TJ

- What POL does well;
- What is at risk;
- What is POL doing about it i.e. mitigating actions;
- When will it be completed by.

AC reiterated that further resource could be provided if required and that due to the varying numbers of standards, one clear view should be established. Any issues should be escalated to him.

He requested a crisper report be published for ARC (29 July) identifying the current position.

4.2 **Cyber Risk Appetite**

AC questioned TJ's request to withdraw the Cyber Risk Appetite paper ahead of the meeting.

TJ commented that following discussions he and RH had had with Shirine Khoury-Haq (NED), and later conversations with JE and David Mann (Head of Information Security & Supplier Risk), it was agreed that the current proposal would be reviewed with further consideration given towards data criticality. An additional request was made to simplify the approach particularly around the key risk indicator element.

AC requested that a real world interpretation should be applied to show POL's risk appetite. He recognised that breaches such as hacking did occur and questioned what would happen to any data lost. JH remarked that whilst a financial penalty was likely and that the regulator (ICO) expected breaches, they expected companies to have established risk processes and controls in place.

The RCC discussed the potential of POL being attacked by hackers and felt that although this scenario was quite low, an attack on Horizon could have significant impact on POL. Having assurance from suppliers about the security of POL's data was critical, especially if POL is the data owner/processor.

Of greater concern to the team was the need to modernise the data centre.

AC thanked the team for their honest assessment and frank conversation. He requested that an updated paper be presented at September's RCC meeting and suggested JE and RH review the scores and the language used. Mitigating actions should also be highlighted/in place.

TJ and TA left the meeting.

5. Transtrack, Back Office Transformation

The paper was taken as read.

BC entered the meeting.

He explained that whilst Transtrack provided POL's supply chain capability for cash and logistics, he questioned the decision to appoint them in 2016 to manage this process.

The financial reconciliation issue (where not all financial transactions recorded in Transtrack are sent to POL's financial system) remained unresolved, but had significantly improved since Go-live, with the team ensuring that financials were robust enough to avoid any branch impacts.

POL00423508

At its peak, around 29,000 transactions (equivalent to IRRELEVANT) had been missed and the project team had now reduced this amount to c.20 missed transactions a day. The bulk of the missing historical transactions had also been processed.

A number of financial controls had been established to prevent further repeated occurrences which had also helped identify any technical issues requiring remediation before they arose. Further, Transtrack had strengthened their team in areas of weakness however it was noted that IRRELEVANT IRRELEVANT

Regarding Back Office Transformation, IRRELEVANT IRRELEVANT

The Committee questioned whether issues how branch incidents were escalated to the RCC but recognised that cultural change was required.

6. Combined Risk, Compliance and Audit Update

6.1 **Risk**

The report was taken as read.

JE reported that the top risks to POL included PCI compliance, the Group Litigation Order, Brexit, People Change and Payzone Payment Device Vulnerabilities.

PCI Compliance

PCI continued to report red. Ingencio had not provided a definitive plan regarding the banking solution and challenge remained with the timeline and costs of the new schedule.

Horizon trial

The second High Court trial relating to Horizon was due to conclude this week (week commencing 1 July). Deloitte had provided support via workshops to identify the risks, mitigation and owners, of the risks raised from the trial. Output from these sessions would be reviewed by Central Risk.

Brexit

Planning remained ongoing with continued and regular dialogue with BEIS. BEIS had confirmed that 'No Deal' plans should be 'shrink wrapped' and that businesses should plan for a 'Deal'. However, JE believed POL should continue to work on contingency plans for 'No Deal' particularly as it was felt the risk for 'No Deal' had not diminished. Brexit (and the associated risks) would continually be reviewed throughout September and October and the Brexit Operations Group would be re-established.

People Change

People change remains a key risk to POL in light of recent significant people changes and future planned organisational changes. The review to assess capability of senior positons including the identification of critical roles continues.

Payzone Payment Device Vulnerabilities

Work to remediate the IRRELEVANT IRRELEVANT continue and are on track. It was expected that remediation would be completed by October from the recent work completed with Payzone and Information Security.

The current exposures were at device level and it was felt that this was holding at an amber position rather than red as previously thought.

BF questioned whether the risk reporting lines for Payzone should report to POL ARC, considering that Post Office Insurance did so. It was noted that whilst Payzone had a risk framework in place, it was not as comprehensive as Post Office Insurance. AC requested JE and BF discuss this outside of the meeting. To do: JE/BF

POL00423508

AC further requested sight of the monitoring data (page 3 of the report) on retail partners and JE proposed that a deep dive be carried out in September. JE to send information to CM. To do: JE/CM

6.2 **Compliance**

The report was taken as read.

Text Relay
POL provided a response to the second part of Ofcom's investigation on 21 June. He noted that Ofcom had recognised the actions POL had taken to date and the commitment to reimburse impacted customers. Where data is available, customers will be reimbursed. Where there is no data, a contribution will be made to Action for Hearing Loss.

GDPR
The programme was formally closed at the end of Q1. Compulsory data protection training has been rolled out for all employees, contractors and agents, with further mandatory training being developed for staff members who have high levels of daily access to sensitive personal data.

Fit & Proper
The team remains focused on gathering F&P returns, with fortnightly updates being provided to HMRC. It was noted that 29 of 43 of POL's commercial partners have responded in full; regarding non-commercial partners, 64% are fully compliant and a further 21% have submitted responses that now require review. A concerted final push is planned for late June/early July for the remainder returns.

A meeting is planned with HMRC next week to discuss the progress made to date, although it was noted that some commercial partners had not responded at all. One solution proposed should no return be forthcoming, is to switch off the branches capability to sell travel money. However he believed this was unreasonable considering HMRC's bill for branch registration fees had recently been paid.

Moneylaundering
The team continued to see a number of high value and complex cases relating to business banking deposits, where deposits are then used to purchase crypto currencies. Concern being the link between crypto currencies and money laundering. IRRELEVANT

IRRELEVANT

JH agreed that for Banking Framework transactions, so long as POL carried out its responsibilities, which it is, the IRRELEVANT However, POL does have duties and is also exposed to reputational risk should POL's network be caught up in money laundering by the banks' customers. It was **AGREED** that a money laundering analysis and risk appetite review should be conducted.

6.3 **Internal Audit**

The report was taken as read.

JA advised that 24 of 26 reviews planned reviews had been completed in the year and that the following recurring control themes had been identified:

- Internal controls not deployed through policies, procedures and systems and/or internal controls not yet designed or operating effectively enough.
- Ineffective identification and/or management of operational, fraud and change risk.
- Unavailability (or ineffective communication) of relevant, quality information to support the internal control function and decision making.
- Lack of clarity of structure, authority and responsibility.

The RCC recognised that progress had been made with regards to reporting clearance lines and the establishment of a clear escalation process to address any significant delays, however report turnaround

POL00423508

(in terms of drafting the report and management review and comment) was below the requested internal service level agreement of clearing audits within 20 days. 10 days was considered ample time in which management should respond.

A number of changes to the content of the IA report summaries was requested by the RCC. These included: To do: JA

- The use of shorter, simpler and clearer report summaries.
- Identifying the severity of any issues raised.
- Providing a broad recommendation such as the development of a new policy/system.
- Identifying whether current policies are suitable for purpose and if so, explaining how they are suitable.
- To have management responses prominently displayed as a headline.

7. Supplier Contracts out of Governance

The paper was taken as read.

The RCC noted that overall, the non-compliance value had dropped slightly since January from IRRELEVANT to IRRELEVANT which was felt to be tolerable risk. The reduction had been primarily driven down by the closure of some material risks through compliant procurement awards, and contracts reaching a statute of limitation on a challenge period.

BB remarked that IRRELEVANT of non-compliance value had been planned/managed over the last six months, however some of this was unmanaged such as the appointment of professional services. She remarked that the risk of non-compliance could be further reduced with the appropriate quote process being used. Additionally, a new panel for procurement was being developed to reduce non-compliance.

The RCC commented that staff should use the CAF process as a matter of standard with appropriate consequences for staff who did not follow protocol.

The RCC requested a number of changes to the format of the report:

- Add a risk indicator to the table of high value open items
- Identify categories of non-compliance
- Remove POI data as this is subject to internal governance only.

BB left the meeting.

8. Business Continuity Update and Policy

The paper was taken as read.

TA remarked that whilst he was happy with the current position, an element of complacency had recently been observed. AC advised that appropriate support would be provided to avoid any slippage.

Evacuation tests had been successfully completed for all sites and IT tested in Swindon was found to be resilient, although he questioned the benefit of moving IT to Swansea. AC requested another evacuation test should be planned for Finsbury Dials.

The RCC requested that the following changes be made to the paper:

To do: TA

- To identify what was currently in place
- To identify what was not currently in place and how this would be fixed
- Description of actions taken to date.

POL00423508

Business Continuity Policy
The Business Continuity Policy was APPROVED for submission to the ARC on 29 July 2019.

TA left the meeting.

9. Policies for Approval

The policies were taken as read.

9.1 **Anti-Bribery and Corruption Review and Policy (including Gifts and Hospitality)**
The Anti-Bribery and Corruption Policy (including Gifts and Hospitality) was **APPROVED** for submission to the ARC on 29 July 2019.

9.2 **Whistleblowing Review and Policy**
The Whistleblowing Policy was **APPROVED** for submission to the ARC on 29 July 2019.

9.3 **Modern Slavery Statement**
The Modern Slavery Statement was **APPROVED** for submission to the ARC on 29 July 2019.

The RCC noted the statement required publishing on the POL website by 1 October 2019, and discussed the volume of work required to meet Section 54 of the Modern Slavery Act 2015.

It was felt that greater communication (to be led by the retail lead team) was required between the network and supplier base to ensure that suppliers were fulfilling their legal requirements. Vetting processes and cultural behaviour would also need to be improved.

JS left the meeting.

10. GDPR Update

The paper was taken as read.

JH reported that the GDPR programme (now closed) had established appropriate controls which gave POL the confidence that operational practices are compliant with GDPR. Some work remained outstanding on:

- contract remediation;
- records retention;
- data classification; and
- data storage.

He commented that the Data Protection Team was confident this work would be completed within the calendar year, and noted that GDPR would be reviewed by Internal Audit in Spring 2020.

The RCC questioned whether POL was fully compliant with GDPR. JH assured the RCC that POL was operationally compliant and could show the regulator (ICO) that established systems and processes were in place.

11. Corporate Insurance Renewal

The paper was taken as read.

The RCC noted the current position regarding the renewal process and that a further update would be provided to ARC in September.

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

POL00423508

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

13. Any other Business

13.1 Meeting dates

It was noted that the next scheduled RCC meeting was on 3 September 2019.

DRAFT

POL00423508

POST OFFICE
AUDIT AND RISK COMMITTEE

PCI Compliance Status Update.

4.1

Author: Phey Rasulian
Date: 29th July 2019

Sponsor: Mark Fabes

Executive Summary

Context

The PCI Programme issued an update to RCC on the 26th June 2019. This paper provides a progress update, specifically progress made with the Point-to-Point Encryption (P2PE) deployment across the pin-pad estate, the preferred approach to the banking and retail transactions processing solution, target operating findings and a timeline to achieve full PCI compliance.

Questions this paper addresses

1. Progress of the Point-to-Point Encryption (P2PE) deployment?
2. What progress has been made to simplify the processing of banking and retail transactions from the pin-pad?
3. What's the outcome of the data audit?
4. Ongoing activities to change the Post Office's operating model to ensure process/procedures are in place to maintain PCI compliance?
5. Whether banking transactions fall under the PCI-DSS governance or should they be considered under an alternative set of regulation?
6. What are the timescales to regain PCI DSS compliance?

Conclusion

1. Point-to-Point Encryption (P2PE) deployment continues on track, with the first tranche of pin-pads due to land in our Milton Keynes branches at the end of August.
2. The preferred solution detail design commenced mid-July after senior-level conversations with Post Office's payment service provider, Ingenico, to request an expedited engagement timeline.
3. The data audit is complete; the findings have minimal instances of PCI-related data. Remediation actions are underway where there is a cost-effective interim solution that can be implemented that does not incur substantial regret spend.
4. The initial analysis of known products and procedures that are within the scope of PCI, to establish their compliance, is well underway. The results to be available at the end of July.
5. Compliance, Legal and Banking teams are exploring if there is an alternative regulation that banking transactions should fall under and not PCI-DSS as banking transactions are not strictly deemed to be payments. No conclusion has been drawn to date; advice has been sought from an external legal counsel.

POL00423508

6. The timeline for regaining PCI DSS Compliance has been estimated to be within the period of Q2 to Q4 2020. These dates are being driven by the delivery of the banking transaction process capability. The programme is working with our partners to expedite the delivery.

Current status

1. Point-to-Point Encryption Deployment

2.1 Work to deploy Point-to-Point Encryption (P2PE) to our pin-pad estate continues with partners, Computacenter/Buybox and Ingenico. A pilot will be conducted at the end of August, and the full rollout will commence swapping out 1000 pin pad per week in September with the deployment concluding in March 2020.

2.2 Post Office's current pin pads have an accreditation expires on April 2020. Post Office has reached out to our card acquirer Global Payments whom in-turn has to reach out to the card scheme's (Visa/Mastercard) for an extension. This is due to a risk that the reaccreditation of the pin pads might not take place before April of next year. Global Payments has confirmed that all card schemes will extend accreditation beyond April 2020, no sunset date has been declared. However there is a further stipulation that remains, that is that the particular model of pin pad in use cannot be installed in new branches beyond April 2020.

2. Preferred Banking Services Solution:

2.1 After the escalation into Ingenico, they have brought forward their engagement by a month. A set of workshops have been scheduled throughout July and August to drive out the detailed design and a refined plan for delivery.

2.2 The team continue to engage with both our Quality Security Assessor (QSA) Nettitude and our Acquirer, Global Payments to ensure our remediation activities will result in required Reports of Compliance, and they support our direction of travel.

3 **PCI Card Data Scan**

3.1 The data scan is now complete, minimal instances of card data were found. A full remediation plan is being created, although certain activities have already commenced.

4 **Target Operating Model**

4.1 The Target Operating Model workstream is analysing all remaining routes for non-compliance and improving the vetting of those activities. These will include but are not limited to, training, change process -incorporate PCI compliance checkpoints. One hundred and three products and seventeen processes are being analysed to establish their PCI compliance status. Currently, out the products and processes identified, sixty-seven products are compliant, thirteen products and five processes have been identified as being non-compliant. The analysis continues, in parallel remedial plans are underway.

POL00423508

5 Should the banking transactions that Post Office process not fall under PCI regulation?

5.1 A request has been issued to explore if banking transactions should be governed under PCI compliance regulation. Post Office has sought external council from Pinsent Mason lawyers and the Payment Service Regulator (PSR) to provide guidance, the feedback is due at the end of July. If the banks were to use the lack of PCI compliance as a reason for not wanting to sign up to banking framework II contract, establishing that Post Office is not obliged to for banking transactions would put Post Office in a stronger position.

6 What is the timeline for regaing PCI-DSS compliance?

6.1 The forecast for regaining PCI DSS compliance's critical path is dependent on the delivery of the new banking transaction processing capability Fujitsu/Ingenico are building for the Post Office. The banking transaction processing capability seems to be the most complex and time consuming deliverable. The estimated window of completion is between Q2 and Q4 2020 currently. The programme will be working with the Post Office's partners to explore any and all opportunities to shotern those timelines however to date, this has been constrained by the availability of key resources from Ingenico. Now that the resources have become available, a plan and costings to deliver all the programme compoents is a high priority.

POL00423508

Cyber Security Update

4.2

Author: Tony Jowett/Jonathan Hill Sponsor: Rob Houghton/Ben Foat Meeting date: 29th July 2019

Executive Summary

Context

In this paper we outline our maturity targets for 2019/20, the steps we have taken to achieve them and plans to complete these actions. We also address how we consider the lessons from external events and threat intelligence to retain our security position.

Questions this paper addresses

- What are our maturity targets for 2019/20 and how did we decide these?
- What is our approach to delivering against these targets?
- What progress have we made in achieving these targets?
- How are we maintain our security posture through learning from external events (including recent data breaches)?

Conclusion

1. The Deloitte Maturity Review produced average benchmark scores for Retail and Financial sectors based on a Global database of maturity scores held by Deloitte. The target scores for Post Office were set by selecting the higher of these benchmarks in most cases, with the lower score being applied to areas that were assessed as less important to Post Office. We now have a set of target scores based on an independent, benchmarked assessment and relevance to Post Office.

2. The Deloitte Review provided current maturity scores which when compared with the target scores gave maturity gaps. These gaps and details of existing Post Office security initiatives were used by Deloitte to form a list of ten key recommendations and over 240 detailed recommendations against all areas assessed. The IT Security Transformation Programme (ITSTP) will deliver the key recommendations and prioritised actions to give the greatest maturity increase.

3. We have completed eight out of ten key recommendations. We have started delivery on the highest priority actions on the detailed recommendations. A plan is included in the Appendix and we expect to reach our target maturity by March 2020 whilst recognising that in subsequent years we will need to continue to deliver security improvements in response to changing business needs and threats.

4. We have onboarded a Cyber Threat Intelligence supplier and ensured closer liaison with the UK's National Cyber Security Centre (NCSC). We are proactively reviewing the recent data breaches from BA, Marriott and Facebook to assess applicability to us and ensure that we learn any relevant lessons from them. We are implementing a quarterly targeted independent red-team investigation into different areas of Post Office.

Input Sought

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

POL00423508

Report

What are our maturity targets for 2019/20 and how did decide these?

1. The Deloitte Maturity Review produced average benchmark scores for Retail and Financial sectors based on a Global database of maturity scores held by Deloitte. These benchmark scores are the average of all Deloitte's Maturity Assessments across their global client base and are anonymous.
2. The Post Office is a unique organisation and as such there is no single benchmark that is applicable. However, Deloitte recommended using a combination of Retail and Financial sector average scores in line with Post Office activities to provide a benchmark.
3. Selecting the target maturity is, in essence, setting an overall risk appetite for the organisation. In most cases we have determined that we have a low risk appetite due to the potential for reputational damage with clients (such as British Gas), new banking framework and the increased scrutiny from media and public attention through the GLO. If we had a higher risk appetite, which is often quite hard to define, we would aim for a lower target maturity.
4. Therefore the target scores for Post Office were set by selecting the higher of the benchmarks in most cases, with the lower score being applied to areas that were assessed as less important to Post Office.
5. Appendix A shows the current, benchmark and target scores selected for Post Office.

What is our approach to delivering against these targets?

6. The Deloitte Review provided current maturity scores which when compared with the target scores gave maturity gaps. These gaps and the existing Post Office security initiatives were used by Deloitte to form a list of ten key recommendations and over 240 detailed recommendations against all areas assessed.
7. The IT Security Transformation Programme (ITSTP) is delivering the key recommendations and a prioritised set of activities to meet the target maturity.
8. The type of activities within this work are:
    a. Delivery of the Deloitte Ten Key Recommendations which form the bed-rock of the maturity increase being sought (listed at Appendix B)
    b. Delivery of the additional detailed actions from the Deloitte Cyber Security review. These range from simple changes to process and documentation to enhancement of technical systems. We are implementing the high and medium priority actions of which there are a total of 120.
    c. Delivery of the detailed actions from the recent Deloitte Information Protection Review. 48 actions are being implemented focusing on high and medium priority.
    d. Delivery of Data Loss Prevention tooling to enable Post Office to track data assets
    e. Increasing the reach and maturity of the SOC
    f. Deployment of RSA Archer for increased Governance, risk and controls
    g. Increased 3rd party assessments

POL00423508

9. We are unable to use the Deloitte Cyber Security Framework tool itself to measure our current maturity as this is Deloitte Intellectual Property. To measure progress the ITSTP team have developed our own maturity tracker and we are using this to measure maturity progress. In addition, Deloitte will perform an annual retest of our maturity levels. We are working with the Post Office Internal Audit team to verify the completion of actions.

What progress have we made in achieving these targets?

10. We have included a Gantt chart showing the plan to achieve the ITSTP in Appendix C. We are aiming to hit target maturity by March 2020. In subsequent years we will need a rolling programme of security improvements to keep Post Office safe in response to developments in the business, the changing nature of the threats faced and the opportunities arising from developments in defensive technology.

11. The **Key Recommendations** are shown in Appendix B. We have completed 8 of these with sign off from Internal Audit. The status of the remaining Key Recommendations is as below.

Recommendation	Action to complete	Target Date
Confirm Cyber risk appetite	Complete risk appetite statements in conjunction with Risk team	ARC Sign off September 2019
Fully document BCM Processes and Procedures	In progress	Q2 2019

12. The status of the remainder of the programme is as follows:

Area	Target Completion	Actual Completion	Completion Date	Next Steps
Deloitte Cyber Review Actions	30%	48%	March 2020	Continue as planned. Key areas where improvements have been made include incident and crisis management, IRRELEVANT IRRELEVANT
Deloitte IP Review actions	30%	30%	March 2020	Continue as planned
RSA Archer implementation	15%	3%	January 2020	Now in mobilisation – delayed due to delay in organisation blueprint delivery. Now rectified.

POL00423508

DLP	-	-		Mobilisation phase – detailed planning in progress – stats required once detailed plans are in place.
SOC Maturity	Treated as ongoing continual improvement to BAU. Widening coverage of SOC through acquisition of more logs including Payzone and Post Office Insurance.			

13. Based on this assessment the gap between the current and target maturity levels of Post Office has been reduced by 23% since the start of the programme in March 2019.

14. 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 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 (and their own suppliers') security risks.

15. 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.

How are we staying agile and learning from external events?

16. To stay focused on current risks we have taken onboard a Cyber Threat Intelligence supplier – IRRELEVANT The RF tool scans the web searching for any mention of Post Office interests and automatically alerts Post Office security to potentially harmful threats. Over the past year RF assessed Post Office to be vulnerable to:

- IRRELEVANT

17. We have established a working group to explore greater use of this data with other Post Office areas such as Brands, Legal, Fraud, Risk, Data Protection to establish a coordinated response cyber threats.

18. We have also sought closer liaison with the UK's National Cyber Security Centre (NCSC) as per a recent email to GE and ARC members. NCSC are able to alert us to active threats and provide cross industry information sharing on key risks.

19. The red-team exercise in 2018 produced useful insight into Post Office's cyber defences. We are not embarking on a programme of targeted red teams aimed at specific areas of Post Office with the first one to be aimed at Post Office Insurance in Q3 2019.

20. The outputs from the above activities will be brought to the Information Security Council (the governance forum for Cyber in Post Office) to determine what changes need to be made to business as usual activities and the ITSTP. If there are more urgent concerns, such as an active threat targeting Post Office, then the cyber incident management process will be invoked.

POL00423508

What has happened in recent data breaches that has resulted in significant penalties from data security regulators in the UK and USA and what is our response?

NB : We describe the details of the breaches that we have below and our response to these is at the end

BA data breach

21. On 8th July, the Information Commissioner's Office ("ICO") announced that it was intending to fine BA £183.39M for "infringements" of GDPR. The proposed fine relates to a cyber incident notified to the ICO by BA in September 2018. Personal data of approximately 500,000 customers were compromised in this incident, which is believed to have begun in June 2018.

22. The ICO's investigation found that a variety of information was compromised by poor security arrangements at the company, including log in, payment card, and travel booking details as well name and address information.

    a. As well as customers' personal details and credit card numbers being stolen, the hackers were also able to scrape the three / four digit card security codes (CVV). PCI DSS requires that CVVs are not be stored on merchants' websites.

23. Although not confirmed publicly, our understanding is that a 'skimming' script had been injected onto BA's website via a weakness in BA's web security that allowed data to be scraped from online payment forms as soon as the passenger pressed the submit button.

24. We believe that at the time BA were in discussions with a major IT supplier to move to a managed service as, allegedly, it was aware that its cyber defences were insufficient to meet GDPR standards.

Marriott International data breach

25. Following fast on the heels of the BA fine, on 9th July the ICO announced its intention to fine Marriott International £99.2M for significant GDPR failings.

26. Marriott notified the ICO in November 2018 of a cyber incident relating to c.339 million customer records, of which approximately 7 million related to UK residents.

    a. The hacked database contained information on guests who had made a reservation at a Starwood hotel including names, addresses, phone numbers, email addresses, passport numbers, DoB, gender, arrival and departure information, reservation dates and communication preferences.

27. It is understood that the breach began when the systems of the Starwood hotels group were compromised in 2014. Marriott subsequently acquired Starwood in 2016, but the exposure of customer information was not discovered until 2018. The ICO's investigation found that Marriott failed to undertake sufficient due diligence when it bought Starwood and should also have done more to secure its systems.

Facebook alleged data breaches / misuse

28. On 12th July 2019 both The Wall Street Journal and Washington Post reported that the Federal Trade Commission ("FTC") approved by a 3-2 vote to fine Facebook c.US$5BN to settle an investigation into the company's privacy violations that was launched following the Cambridge Analytica revelations. It is expected that the US Department of Justice will approve the fine.

    a. Neither the FTC nor Facebook have commented on the reports

POL00423508

29. The US investigation looked into alleged breaches of privacy against users' accounts and the lack of security controls to prevent 'rogue states' / organisations manipulating data and feeds to potentially sway democratic processes both in the US and the UK.

    a. The allegations are that Facebook inappropriately shared with Cambridge Analytica the personal data of c.87 million users without their knowledge or consent. This broke a 2011 agreement Facebook signed, protecting the personal data of its users.

    b. Although the findings of the investigation have yet to be made public it is believed that poor security controls allowed Cambridge Analytica access to the bulk data, which it was then allegedly able to use to create manipulate live feeds through to Facebook users with the intention of swaying voting preferences within the US elections. It is further believed that this may have occurred in the UK, although to date no evidence has been published proving this.

30. It is anticipated that the ICO is due to release details of its own finding shortly.

Post Office Response to Breaches

31. We have end to end security controls which seek to address the risk of such breaches. The ITSTP is strengthening these in line with our target maturity as described previously in this report. We don't believe we are open to these specific incidents, but we are taking a series of risk mitigating actions to ensure that we are not vulnerable to them.

32. Further actions being taken in response are:

    a. We have asked NCSC to share any details they have regarding the nature of the breaches so that we can be as specific as possible in improving our own defences.

    b. In response to the BA and Marriott breaches we have sent a letter to our major 3rd party vendors asking for assurances from them that, where they hold personal and other sensitive data on behalf of Post Office that a similar incident could not happen to us. A response is expected by 26 July 2019

    c. We have instigated a review of penetration test results to double check the execution of **IRRELEVANT**
    This will be complete by 2 August 2019

    d. As mentioned previously in this report we are instigating a quarterly series of red-team tests to gain further assurance that our controls are strong enough and to address any identified weaknesses in our response. This will be conducted across Post Office and will include Post Office Insurance and Payzone. The first one will be during August and will be carried out in Post Office Insurance.

POL00423508

Appendix A Maturity Scores with Target maturities for 2019/20

Summary Scores

Domain	Sub-domain	Capabilities	Phase 1 Un-validated Maturity Score	Phase 2 Validated Maturity Score	Average Maturity (Global Retail)	Average Maturity (Global Financial Services)	POL Endorsed Target Maturity
Governance	Cyber security management	Strategy & operating model	IRRELEVANT				
		Policies, standards & architecture					
		Cyber risk culture and behaviour					
		Cyber risk management, metrics & reporting					
Secure	Extended Enterprise and Infrastructure	Cloud security					
		Third party risk management					
	People & Workplace	Human resources security					
		Physical security					
	Identity & Access management	Identity lifecycle management					
		User access control					
		Role based access control					
		Privileged user access control					
	Applications	Secure Software Development Lifecycle					
		Post-development application protection					
	Infrastructure	Asset management					
		System security					
		Malware protection					
		Network security					
		End-user device security (CD)					
	Data	Data loss prevention					
		Encryption					
		Information lifecycle management					
		Data privacy					
		Information classification					
Vigilant	Vulnerability identification	Penetration testing & vulnerability scanning					
	Threat Intelligence	Cyber threat intelligence (CTI)					
		Brand protection					
	Security Operations (SOC)	Security event monitoring					
		Patch & vulnerability management					
		Cyber analytics					
		Security platform administration & operations					
Resilient	Incident management	Incident & crisis readiness					
		Incident response					
	Business Resilience	Business continuity management and recovery					

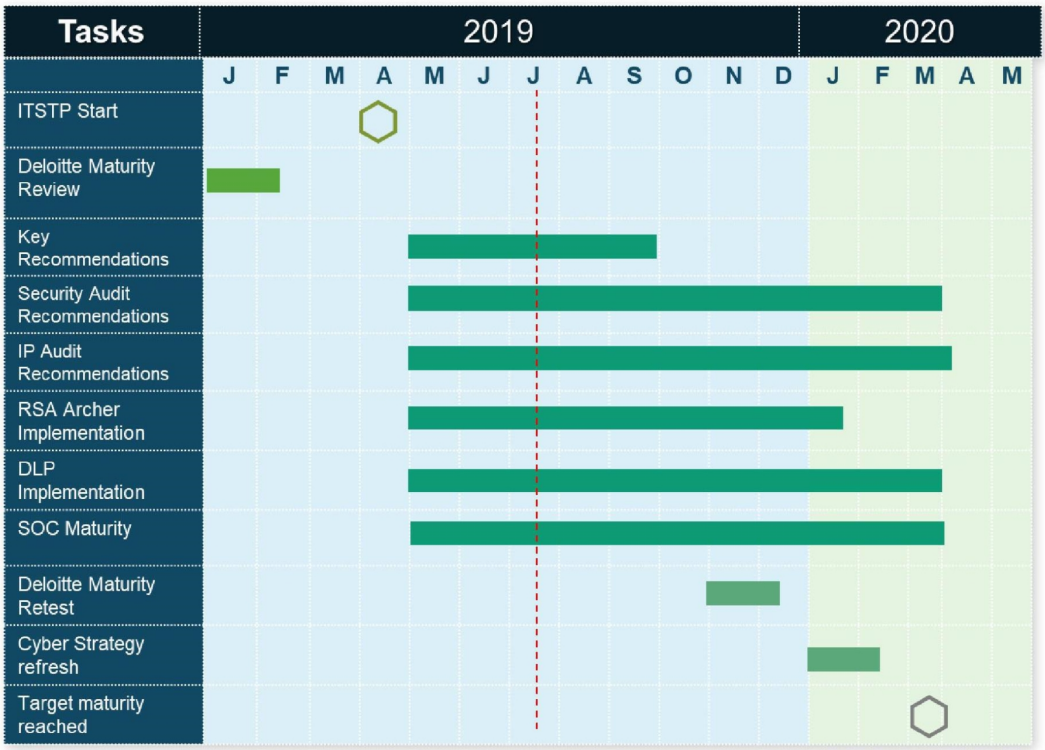
POL00423508

Appendix B Deloitte Key Recommendations

1. Confirm Principal IT risks and risk appetite statements (specifically including the Cyber Security risk)
2. Create a prioritised list of crown jewels.
3. Agree target maturity levels for all Cyber Security domains.
4. Perform a gap analysis between the IT Security Transformation Programme (ITSTP) and the recommendations from this review
5. Update the ITSTP to address any gaps from the gap analysis.
6. Implement a mechanism to track and report progress against the ITSTP
7. Review, finalise and share cyber risk metrics with a view to regularly reporting a dashboard to the Board.
8. Develop Post Office's Cyber Threat Intelligence (CTI) capability in order to proactively inform decision making across the business by agreeing a framework for CTI.
9. Develop Post Office's Resilient capability by fully documenting BCM procedures and processes in respect of cyber resilience
10. Develop and agree an Insider Threat Programme

POL00423508

Appendix C ITSTP 2019/20 Plan



POL00423508

Annual Report and Accounts – GLO & Starling

Author: Ben Foat, General Counsel Sponsors: Al Cameron, Interim CEO Date: July 2019

Executive Summary

Context

Post Office is required to lay its accounts before Parliament and is required to provide an Annual Report and Accounts (ARA) for each financial year. In doing so, Post Office needs to consider the accounting treatment of the Group Litigation and Starling "workers rights" claim in respect of accounting regulatory requirements contained in IAS 37 *Provisions, Contingent Liabilities and Contingent Assets.* This paper is subject to legal privilege and should not be used, disclosed or forwarded for any other purpose.

5

Questions this paper addresses

1. What are the accounting requirements of IAS 37?
2. What provision or disclosure should the Post Office make in respect of Project Starling in the ARA?
3. What provision or disclosure should the Post Office make in respect of the Group Litigation in the ARA?

Conclusions

1. Post Office is required to make a provision in the accounts if it has a present obligation as a result of a past event where it is probable that an economic outflow will occur **and** that a reliable estimate can be made of the amount of that obligation. If on the other hand, there is only a possible economic outflow then a contingent liability disclosure statement should be contained in the ARA. Appendix 1 summarises the relevant sections of IAS 37. Appendix 2 summarises the disclosure requirements of IAS 37 in respect of contingent liabilities.
2. IRRELEVANT
3. It is recommended that ARA contains a contingent liability disclosure statement as set out in Appendix 4 in respect of the Group Litigation on the basis that it satisfies the contingent liability test and it is not practicable at this to provide a reliable estimate at this time.

Input Sought

The Board is asked to note the accounting requirements and approve:

1. IRRELEVANT
2. Making of an contingent liability disclosure statement in the ARA in respect of the Group Litigation in the terms set out in Appendix 4.

Legally Privileged and Strictly Confidential

POL00423508

The Report

Starling

IRRELEVANT

5

Legally Privileged and Strictly Confidential

POL00423508

IRRELEVANT

5

Group Litigation

The Group Litigation comprises 555 claims against Post Office currently being heard over at least 4 series of trials. Several board papers on the Group Litigation have been provided to Board and a further updated GLO report has been provided this month.

No legal liability

At this stage, the Court has not yet made any determination of liability or assessment of the claim value. There is presently no legal liability. The Post Office was however mostly unsuccessful in the common issues trial and Justice Fraser has been highly critical of Post office and the conduct of the litigation. An appeal, however, has been lodged on most of the legal points that Post Office lost and we are waiting to hear if permission to appeal will be granted. The view of previous Counsel, David Cavender QC, was that Post Office should be successful on most of the points being appealed. New Counsel has now been instructed, Helen Davies QC, and she will be providing a fresh opinion on this if permission to appeal is granted.

The second trial which focused on Horizon closed on 2 July and will determine 15 issues about the functionality and reliability of the Horizon system across the Post Office network. The advice of Leading Counsel for Post Office on the Horizon Issues trial, Anthony de Garr Robinson QC, is that the judgment is likely to be adverse to Post Office, though the precise findings are difficult to predict. Justice Fraser has indicated that a judgment is not likely before mid-September. A third trial to consider "Further Issues" has been moved back to March 2020. The Further Issues address the breach and

POL00423508

limitation claims in two test cases, with the objective of setting down decisions that could then potentially be applied across the wider group given that around 350 Claimants' claims are potentially subject to full or partial limitation defences. If a full limitation defence is established in any particular case that Claimant's claim should be rejected entirely. A fourth trial was scheduled for March 2020 but will now be pushed back and the scope of that trial is not currently set. Beyond the Fourth Trial there is the potential for further trials.

On a strictly legal assessment there is no probable economic output given that leave to appeal the common issues judgement is being sought; the horizon judgement has not yet been handed down and in any event it would not produce any legal liability; and there is no actual legal liability against Post Office as at this time.

Probable Economic Outflow from Settlement

However, in light of common issues judgement and broader commercial considerations, the Post Office's new strategy is to seriously consider alternative dispute resolution through mediation. It has written to the Claimants' solicitors seeking a mediation. This could mean that there will be a probable economic outflow within this financial year.

Each of the 555 Claimants has filed a Schedule of Information (**SOI**), which describes their individual claim at a very high level. Only six Claimants have filed individual Particulars of Claim (though these do not describe their full claims as that was not required by the Court) and handful of other Claimants have filed witness statements that provide a limited insight into their claims. Post Office also has information from some of the Claimants through the mediation scheme but that information is now 5 years old.

At a Court hearing last year, the Claimants' Counsel stated that, for cost budgeting purposes, the claim was worth £80m - £90m, but this figure was never explained or substantiated despite requests to do so. The SOIs contain some quantification of some heads of claim. If taken on face-value, the 555 claims add up to £224m. However, the view of Post Office's external solicitors, Womble Bond Dickinson (**WBD**), is that this figure is unreliable in that it both overstates and understates the true claim value. For example, the SOIs did not require the Claimants to value certain types of loss; personal injury and reputation damage being the main ones. Also, the Claimants have claimed for losses, particularly loss of earnings that exceed what one would expect to be recoverable on normal legal principles. For example, £150m of the £224m figure is claimed on the basis of loss of earnings post termination and it is the claims which span from termination until retirement age which generate the large quantum claims. Overall the quality of the SOIs is quite poor which also makes them a questionable source of information. At this stage, WBD's view is that there is no reliable valuation of the claims available.

Although Post Office is seriously considering alternative dispute resolution options which may very well result in a probable economic outflow, there are a number of barriers to settlement. The key ones being:

- We do not know the Claimants' expectations for settlement or whether they are even prepared to settle.

POL00423508

- The lack of a reliable claim valuation. WBD has, based on the information presently available, prepared an initial assessment of a possible settlement range, being £38m to £84m, but this is heavily caveated and subject to a wide margin of error.

The Judge has indicated that he intends to make costs awards at the end of each trial rather than reserve costs to the end of the litigation. He has ordered Post Office to pay the Claimants' costs of the Common Issues trial, with a payment on account of £5.5m. Various other costs orders have been made on other interim applications and hearings. Further costs orders are expected to follow the Horizon and Further Issues trial.

Reasons for not making a provision

IAS 37 states that a provision should only be recognised when all of the following criteria are met:

(a) an entity has a present obligation (legal or constructive) as a result of a past event;
(b) it is probable that an outflow of resources embodying economic benefits will be required to settle the obligation; **and**
(c) a reliable estimate can be made of the amount of the obligation.

Whilst management recognises that the advancement of the new strategy means that it is possible that economic flow may occur later this year if settlement can be achieved, a reliable estimate cannot be made of the amount of the obligation at this time.

Moreover, the factors against making provision include:

- No determination of liability or order for compensation has yet been made.
- Although the Post Office did not succeed in respect of the Common Issues Trial, it does not give rise any liability in and of itself and in any event Post Office is seeking the Court of Appeal's permission to appeal the substantive points.
- At this point of time there is no adverse finding in respect of the Horizon Trial but even if there was that would not result in a legal liability or an obligation to pay (other than costs).
- It is unknown whether the Claimants are willing to settle at this stage and if so for what amount.
- Management view is that the Claimants would not be willing to settle for an amount that Post Office would consider making at this juncture (circa £20m).
- It is unlikely that the Horizon and Further Issues trial will result in orders for compensation.
- The scope and date of the fourth trial is currently unknown (which could result in compensation orders for a small number of Claimants).

POL00423508

- The ultimate liabilities in the litigation will turn on the specific facts and merits of each individual claim (which have not yet been assessed).
- The currently available information on claim value is untested and unreliable. Though the amount claimed is significant, the facts (e.g. that the claimed losses where in fact suffered) and legal basis (i.e. that they satisfy the legal tests of liability, causation, remoteness and mitigation) for such claims are yet to be tested.
- The price of any settlement is partially driven by the objectives and negotiating position of the Claimants and these are currently unknown.

Recommendations

It is recommended that the ARA contains:

1. IRRELEVANT
2. a disclosure statement as set out in Appendix 4 in respect of the Group Litigation on the basis that the test for a provision has not been satisfied for the reasons given above but it satisfies the contingent liability test.

POL00423508

Appendix 1: IAS 37 Provisions, Contingent Liabilities and Contingent Assets

- 7.1 Definitions:
  - i. A provision is a liability of uncertain timing or amount.
  - ii. A contingent liability is a possible obligation or present obligation that is not probable or not reliably measurable.
- A provision should only be recognised when:
  - i. an entity has a present obligation (legal or constructive) as a result of a past event;
  - ii. it is probable that an outflow of resources embodying economic benefits will be required to settle the obligation; and
  - iii. a reliable estimate can be made of the amount of the obligation.
- A contingent liability is defined as:
  - i. A possible obligation that arises from past events and whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the entity; or
  - ii. A present obligation that arises from past events that is not recognisable because:
    1. it is not probable that an outflow of resources embodying economic benefits will be required to settle the obligation; or
    2. the amount of the obligation cannot be measured with sufficient reliability.
  - iii. Under IAS 37 an entity should not recognise a contingent liability on its statement of financial position.
- IAS 37:15 states that there will, on rare occasions, be circumstances when it is unclear whether a present obligation exists. In order to determine whether a present obligation exists under such circumstances (e.g. when the facts in a lawsuit are disputed), the Standard advises that account should be taken of all available evidence. Such evidence may include, for example, the opinion of experts. It will also include additional evidence contributed by events occurring after the reporting period. Preparers of financial statements should look at all of the available evidence and come to a reasoned judgement as to whether it is more likely than not that a present obligation exists. If it is more likely than not that a present obligation exists, a provision should be recognised. Otherwise, a contingent liability is disclosed, unless the possibility of any transfer of economic benefits in settlement is remote [IAS 37:16].
- An essential element of the definition of a liability is the existence of an obligation to transfer economic benefits. Recognition of a provision is conditional on the transfer of economic benefits being 'probable'. For the purpose of IAS 37, probable is taken to mean more likely than not to occur [IAS 37:23].
- The amount to be recognised as a provision under IAS 37 is the 'best estimate' of the expenditure required to settle the present obligation at

POL00423508

the end of the reporting period. [IAS 37:36] The reference to the end of the reporting period does not preclude use of later additional evidence or better information, but indicates that the best estimate will be the amount that a reporting entity would rationally pay at the end of the reporting period to have the obligation taken away – by settlement or by transfer to a third party [IAS 37:37].

i. The addition of 'rationally' in IAS 37:37 suggests that, although it may be difficult to arrange settlement or transfer, there is nevertheless a point of balance, and thus a price, at which management, taking all possible outcomes into account, could be willing to settle.
ii. Ultimately, the best estimate will be determined based on the judgement of management and will reflect experience of similar transactions. In reaching that judgement, reports of independent experts may be required. Examples of relevant independent experts are solicitors and barristers.

Appendix 2: Disclosure Requirements for Contingent Liabilities

- For each class of contingent liability (unless the possibility of an outflow in settlement is remote), a brief description of the nature of the contingent liability should be provided. The following information should also be disclosed, if practicable [IAS 37:86]:
  i. an estimate of its financial effect (based on the measurement requirements of IAS 37);
  ii. an indication of the uncertainties relating to the amount or timing of any outflow; and
  iii. the possibility of any reimbursement.
- In extremely rare cases, it is conceivable that some or all of the disclosures required by IAS 37 can be expected to prejudice seriously the position of the entity in a dispute with other parties on the subject matter of the provision, contingent liability or contingent asset. In such cases, the reporting entity need not disclose the information, but it should disclose the general nature of the dispute, together with the fact that the information has not been disclosed and the reason why [IAS 37:92].

Appendix 3: ARA Disclosure – Starling

IRRELEVANT

Legally Privileged and Strictly Confidential

POL00423508

IRRELEVANT

5

Appendix 4: ARA Disclosure – Group Litigation

We have drafted the following disclosure. This disclosure fulfils the requirements of IAS 37 shown in appendix 2.

On 11 April 2016, a High Court claim was issued on behalf of a number of postmasters against Post Office in relation to various legal, technical and operational matters, many of which have been the subject of significant external focus for a number of years.

The litigation is very complex and the Judge ordered that it will be heard as a series of trials.

The first trial, which finished on 5 December 2018, was about determining the legal construction of the contract between Post Office and postmasters. The Judgment from this trial was made public on 15 March 2019. Post Office acknowledges the Judgment and will continue to enhance operational controls and work with Postmasters to ensure that we provide the best service possible to our customers.

On 23 May 2019, the Court awarded the Claimants their costs in respect of the first trial. As a result, Post Office was instructed to make a payment on account of £6 million. These costs have been recognised in 2018/19 as they reflect conditions that existed at the end of this reporting period.

Legally Privileged and Strictly Confidential

POL00423508

The second trial, about technical matters concerning Post Office's Horizon computer system started on 11 March 2019 and concluded on 2 July 2019 when the Judge retired to consider his judgment. The judgment is not expected to be handed down before mid-September 2019.

Neither the first nor second trial have or will determine liability or the individual claimants' cases. A further third trial are scheduled for March 2020 but the fourth trial has not yet been set down.

To date, the Claimants have not asserted the aggregate value of their claims in any of the Particulars of Claim filed in the litigation.

While the Directors recognise that an adverse outcome could be material, they are currently unable to determine whether the outcome of these proceedings would have a material adverse impact on the consolidated position of the Group, and are unlikely to be able to do so until the Court has made further determinations and the Claimants have provided the necessary information about the value of their claims. The Directors continue to keep this under close review.

The Post Office Group Litigation represents a possible obligation arising from past events, whose existence will be confirmed only by the occurrence or non-occurrence of one or more uncertain future events not wholly within the control of the Group.

The costs of IRRELEVANT included in exceptional items relate to Post Office defending the Post Office Group Litigation IRRELEVANT during the financial year.

POL00423508

Risk, Compliance and Audit Report

Author: J Ellwood, J Hill, J Appel Sponsor: Al Cameron/Ben Foat Meeting date: 29 July 2019

Executive Summary

Context

This paper provides an update on the key and emerging risks, compliance matters that Post Office is managing and an update on the latest Internal 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?

6.1

Conclusion

- There has been no significant change in our risk profile, with continuing focus on Litigation, PCI compliance, Brexit and the retention of key people.
- The change portfolio remains Amber and is contributing a higher proportion of Internal Audit findings. A new Transformation Director has been hired because it is clear that changes made last year have not brought the required level of control.
- Updated training on GDPR is live for our people and we are improving compliance with Fit and Proper and Money Laundering. Fit and Proper will require us to switch branches off until they have completed the process to ensure full compliance.
- Mystery Shopping results remain a concern and may have suffered from the recent restructuring. Actions to improve performance are now being implemented, including updated training for new Area Managers, reduced ratios of CRMs to AMs and increased support from Compliance.
- Eight internal audits have been completed, bringing us up to date and completing the 2018/19 work. There were no adverse rated reports. One out of 79 open actions was overdue.

Input Sought

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

POL00423508

The Report

Risk

Author: Jenny Ellwood

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

1.1. Legal and Regulatory and Strategic are the principal risk categories which continue to report red on the heatmap (see Appendix 1 in the reading room) and where there is continued focus on actions.

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

6.1

1.3. The PCI risk continues to report red (4:4) and a separate update from IT will be provided in the meeting. Key points to draw out are there have been challenges with Ingenico regarding timeline and cost of the new solution. After executive level escalations Ingenico have expedited their engagement and design activity is to start week commencing 22 July, which will determine prices and timescale. In addition to this, the pin-pad preparation and rollout activities are on schedule with the first refreshed pin-pads arriving in branch at the beginning of September.

1.4. 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). 8 of 10 'high-rated' recommendations have been closed. The other 2 remain on track.

1.5. The second High Court trial relating to Horizon has concluded with the outcome anticipated in early September. Deloitte are supporting Post Offices preparations and workshops continue to record the risks, mitigations and owners. Central Risk will review the outputs from these sessions.

1.6. 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, which was ratified in the Cyber Risk Workshop which took 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.

1.7. A wider risk workshop to consider other risk areas i.e. strategic, operational and financial and to help build Payzone's risk management framework and governance has been arranged for 30 July.

POL00423508

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

1.8. In terms of the commercial risk called out in May regarding Fit and Proper, the compliance section confirms the latest position (Para 2.12). Work is continuing to obtain the registrations. It is anticipated that there will be some agents where this is not received and letters will be sent in advance to confirm next steps. This could encourage agents to complete the registration and further reduce any de-registrations required.

1.9. 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.

1.10. 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.

1.11. Brexit planning continues and we remain in regular dialogue with BEIS. BEIS await the announcement of the new Prime Minister and the Secretary of State. Once this is announced they anticipate work to reconvene in vigour. From a Post Office perspective we continue to work on remediation activities for a 'No Deal', particularly the ongoing engagement with third parties who have not yet responded to our questionnaires. The Operations Working Group is to be re-established to review our original contingency plans and agree and progress any new actions. We need to also consider activities such any major 'IT' releases or significant marketing campaigns during the lead up to the 31 October and the immediate time after which may create additional pressures.

1.12. 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 been developing MI and a draft scorecard. The multiples to be monitored initially are: McColls, Cooperative, WH Smiths, AF Blakemore, One Stop and Tesco and additional partners can be added based on size or risk. Retail will bring the MI and approach to Septembers RCC for review and ratification.

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

1.13. 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.

POL00423508

1.14. 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.

1.15. Within the reading rooms a summary of the current key 'Platinum and Gold' change programmes and their current reporting status has been uploaded (Appendix 3). Four projects are reporting Red RAG statuses, two of which relate to Project Leo and PCI, which this committee are receiving updates on. Of the remaining two there is only one which we believe ARC should have awareness of:

- **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.

1.16. The June Change Risk Management Group (CRMG) considered the existing eight strategic portfolio risks. There are no new risks to escalate and the strategic portfolio office continue to mitigate the People risk which is still scored as a (3:4) and has previously been reported through to ARC. A key mitigation is enhancing the competency levels of both the permanent and contractor Change staff. A competency framework has been developed and will be used to assess the level of competency of existing staff and ensure new recruits meet the required standards.

Compliance — Author: Jonathan Hill

Telecoms

Text Relay

2.1 We continue to work with Ofcom on its investigation. Ofcom has advised that it will be sending a further S135 information request to seek more information on the data we provided and also evidence as to when senior managers were informed about the text relay issue and the action they took.

2.2 All impacted customers who are still with Post Office Telecoms were given compensation via a credit on their bill (IRRELEVANT) while ceased or inactive customers were sent a letter and a cheque (IRRELEVANT). Where we do not have data we will make an estimate and then make a contribution to our selected charity, Action for Hearing Loss.

Age Verification for Online Adult Internet Sites

2.3 On 20th June the Secretary of State for BEIS announced that the Age Verification requirement had 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.

POL00423508

Data Protection

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

2.5 This year's Data Protection training has gone live for all employees, contractors and agents. Additional mandatory training is in development for those employees that use or have access to bulk and/or sensitive personal data such as HR, Marketing and the IT community.

2.6 There have been two Privacy and Electronic Communications Regulations notifications outside of the statutory 24hr reporting period which may result in a fixed penalty notice of (£1,000). These were attributed to agent error within the Telecoms Call Centre. In response additional training has been rolled out and new controls deployed which underwent UAT week commencing 1st July 2019.

Financial Crime

Compliance with Money Laundering Regulations

2.7 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.

2.8 Resource provided by the Data Centre of Excellence to resolve outstanding issues with the Bureau de Change transaction monitoring system has delivered a number of the additional reports that had been agreed with HMRC. We are piloting these and have identified some branches where high levels of cash purchases just below £1,000 are indicating deliberate avoidance of customer data and ID capture requirements. The reports and will be tested over the next 6 months.

2.9 There remains an outstanding AML Credence architecture issue that is causing transaction record errors for certain declined transactions. This is with Accenture to implement a fix. This issue does not impact Horizon or any other core Post Office systems – it is limited to the branch bureau data copied into AML Credence.

Anti-Bribery and Corruption ("ABC") update

2.10 Please see separate report.

Whistleblowing update

2.11 Please see separate report.

POL00423508

Fit and Proper

2.12 Focus on gathering agent F&P returns continues and we are sharing data with HMRC fortnightly to evidence our progress:

- We expect all Commercial Partners will achieve full compliance, although some chasing is still required
- For all other agents, 68% are fully compliant and 17% have submitted responses which need work but are expected to achieve compliance by end July. Letters to the partial-responders / non-responders have been sent, advising a final deadline of 23rd August 2019 and that non-response will result in Travel Money and MoneyGram services being switched off on 30th August 2019
- These remaining agents have been assessed High, Medium and Low priority (based on volume and value of sales), with 'High' being contacted by Network Area Managers, and the remainder contacted by the F&P team in Chesterfield.
- The revoke functionality (MDM and Horizon) and the accompanying operational processes are being reviewed and refined to enable agents complying after 23rd August to be easily re-instated.

2.13 The processes and systems changes required for ongoing annual F&P declaration from January 2020, are being developed and agent annual declarations will be spread throughout each year.

Regulatory updates

2.14 Post Office submitted a response to the HMT consultation on the transposition of 5th Money Laundering Directive into UK law. Amongst other matters where we are seeking clarification, 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.
- we are also asking the Government to recognise GOV.UK Verify scheme under the provisions

External Threats

2.15 We continue to see a growing number of high value and complex cases relating to business banking deposits. HMRC has presented a case arising from Post Office-submitted SARs, to the UK's Joint Money Laundering Intelligence Taskforce (of which we are a member) highlighting evidence that IRRELEVANT

IRRELEVANT

2.16 We are conducting a review of AML/CTF risk appetite as a result of the growth in banking framework transactions, the high number of investigation cases and the increased interests from regulators (e.g. HMRC, PSR, BoE and Treasury).

POL00423508

Internal Threats

2.17 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.

Supply Chain Compliance

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

Financial Services

Credit Cards

2.19 The Post Office - Capital One Marketing Services Agreement and the Appointed Representative Agreement (ARA) have now been signed. This requires 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.

2.20 Following the agreement on the ARA we will need to put in place a Regulatory Guidance Manual that outlines the key responsibilities Post Office has to put in place to maintain compliance, including financial promotions approval processes.

Current Account Withdrawal

2.21 We are monitoring the withdrawal with BoI. As at end of June c.41% of the book had closed or switched (10 thousand customers, reducing balances from **IRRELEVANT** in line with BoI's forecast.

- The FCA is aware of the withdrawal and is comfortable with the process and how customer will be treated after inactive accounts have been closed on 11th September 2019.
- Active accounts will not be closed until at least 11th November. However, they will not be able to access Internet Banking. Branch services will still be available.
- A 3rd party agency is being tasked by BoI to find customers between September and November who have not contacted BoI. Post 11th November, BoI will continue to deal with customers who contact them and return funds.
- Overall, we have had 120 complaints regarding the decision, 87 complaints regarding the closure process and 90 complaints regarding switching delays

Mystery Shopping Results

2.22 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

POL00423508

condition status. Training is being provided in Q2 to align with the summer period

2.23 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

2.24 We are working with the Network teams on the changes they are making to their branch management approach, including CRMs with the aim of maintaining appropriate oversight and conduct management whilst reducing the T&C burden on the teams. An update on the agreed solution has been shared with both Principals and we continue to provide regular updates. The improvement action plan is included in the Reading Room.

Vulnerable Customers

2.25 The Vulnerable Customer Module and test was launched on Success Factors on 20th May, supported by Team Talks in the Network and awareness packs for Area Managers to brief Postmasters.

2.26 An external accessibility expert Kate Nash Associates has completed the review of our Post Office 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) Loyalty Penalty Super Complaint to the CMA

2.27 The Secretary of State for BEIS wrote to the Chief Executive of the CMA on 19th June strongly supporting the findings of the super complaint. The Government has 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.

2.28 BEIS proposes 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. The CMA will consult on how best to achieve this although it is not expected to intervene in areas already regulated by Ofcom and the FCA.

POL00423508

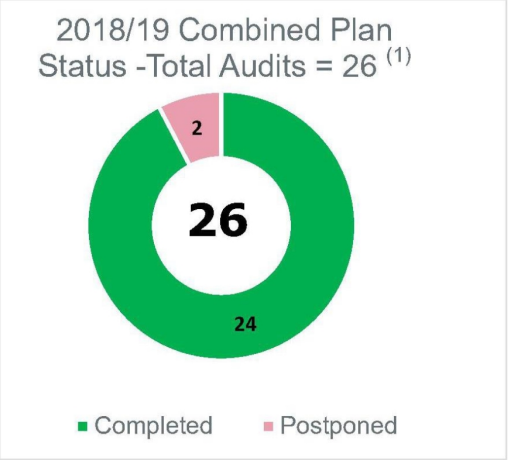
Internal Audit Author: Johann Appel

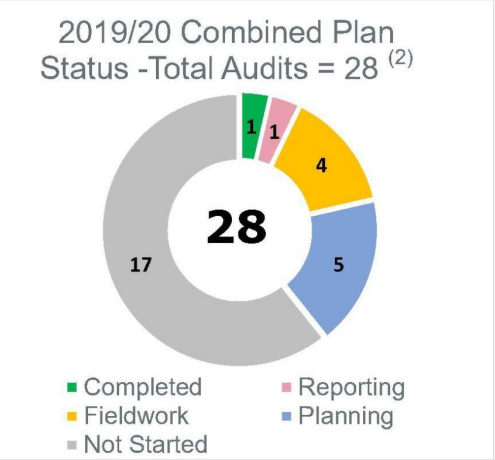
Progress against plan:

3.1 Eight reviews have been finalised since the May ARC, with summaries included in paragraph 3.10

3.2 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.

3.3 Delivery of the 2019/20 programme is progressing well.





(1)ARC approved baseline plan for 2018/19 (16 core internal audit reviews & 10 change assurance reviews).
(2)ARC approved baseline plan for 2019/20 (18 core internal audit reviews & 10 change assurance reviews).
Details of the audit plan status for both years are included in the reading room (appendix 5).

Internal Audit reviews in progress and planned for delivery in Q2

3.4 The following reviews are being planned for delivery in Q3 (A full summary of the 2019/20 audit plan status is included in the reading room as appendix 5):

	Review	Status	Timing
1	Procure to Pay	Fieldwork	24/06 – 15/08
2	Data Analytics Excellence (Change)	Reporting	12/06 – 15/07
3	Effectiveness of Gating Ph1 (Change)	Fieldwork	12/07 – 08/08
4	Effectiveness of Second Line Assurance Ph1 (Change)	Fieldwork	12/07 – 08/08
5	Benefits Realisation Ph1 (Change)	Fieldwork	12/07 – 08/08
6	Investment Funding Controls (Follow-up)	Planning	05/08 – 30/08
7	Payzone Internal Controls 'Health Check'	Planning	15/08 – 15/09
8	Employee Expenses Follow-up	Planning	26/08 – 30/09
9	Telco Billing Process	Planning	August
10	Payment Technology Upgrade (Change)	Planning	Sept

POL00423508

Summary of Control Themes and Root Causes for 2018/19:

3.5 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 five control themes were as follows, with full results included in the reading room (appendix 6).

Control Theme (by COSO control components)	18/19	17/18	
Change Delivery[3]: Ineffective change governance, risk management and tracking / realisation of benefits.	43%	29%	↑
Control Activities: Internal controls are not deployed through policies, procedures and systems and / or internal controls are not designed or operating effectively.	16%	33%	↓
Information & Communication: Unavailability of relevant, quality information to support the internal control function and decision making.	12%	7%	↑
Risk Assessment: Ineffective identification and/or management of operational, financial and information risk (including unclear expression of risk appetite).	5%	10%	↓
Risk Assessment: Direction of travel and strategy is not clear.	5%	1%	↑

[3] Change Delivery is not a standard COSO component, however, these findings are shown separately to avoid distortion of BAU controls. Numbers for 2017/18 were restated for comparison.

3.6 The year-on-year movements in control themes can be summarised and interpreted as follows:

- Change Delivery: A significantly higher number of control failings were identified compared to the previous year, despite a lower number of reviews performed. Portfolio level controls have started to improve, however, there appears to be a lag in adoption of these controls at programme level and/or controls are not sustainable. The recent reorganisation of the portfolio office and appointment of new Chief Transformation Officer is expected to improve the management of change risk.
- Control Activities: The percentage of audit findings relating to ineffective control activities has reduced by 17 percentage points, indicating that operational controls are improving or maturing. The continued development of the Financial Control Framework and implementation of the IT Control Framework appear to have contributed to this significant improvement. We recommend that management roll out similar control frameworks to formalise controls in other parts of the business, e.g. Operations and HR.
- Information & Communication: 12% of control failings could be attributed to lack of correct and up to date information, or ineffective communication (increase of 5 percentage points).
- Risk Assessment: Although operational risk management improved, this was offset by less effective risk management at strategic level (unclear strategy and direction of travel).

POL00423508

Report turnaround:

3.7 The average time to clear internal audit reports was 41 days against a target of 20 days. We have taken steps to make clearing of reports 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 prevent 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.

Status of Audit Actions:

3.8 A total of 271 audit action were raised during 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 19 July 2019 there were 79 open actions, 1 of which was overdue.

Audit Action Status:	
Open (not yet due)	78
Overdue (<60 days)	1
Overdue (>60 days)	0
Total	79

Internal audit reviews completed

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

1	IT Control Framework		5	Pensions Follow-up (2019/20 plan)	
2	IT Contract Management		6	Change Excellence (Follow-up)	
3	FS Training		7	P2C Belfast Exit	
4	Payroll		8	Payzone Integration (Panther)	

3.10 Our findings and observations from these reviews are summarised below, with the full reports available in the reading room:

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



Needs Improvement

Sponsor:
Rob Houghton

Audit findings:

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 recommended some actions to enhance the ITCF, including:

- Establishing a formal activity to develop and refine processes and controls;
- Enhanced communication & training;
- A more fully featured tool to support the ITCF
- Improved management information over operation of the ITCF; and
- 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.

POL00423508

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



Sponsor:
Rob Houghton

Audit findings:

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 2018 and will also inform a review of Post Office wide contract and vendor management (CVM) processes, which is planned for 2020/21.

The review highlighted the lack of an owner at GE level for Post Office wide 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.

Despite the absence of a Post Office CVM control framework, 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.

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."

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



Sponsor:
Debbie Smith / Owen Woodley

Audit findings:

P1	0
P2	1
P3	1
Total	2

POL has a regulatory responsibility, via its AR agreements, to put effective systems and controls in place by which colleagues introducing and selling 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.

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.

POL00423508

Payroll Process (Ref. 2018/19-18)



Sponsor:
Mo Kang

Audit findings:

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 for remediation:

- 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 is largely avoidable (IRRELEVANT).
- There is inadequate segregation of duties, which are partly caused by the overlapping of role based permissions.
- IRRELEVANT

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 data analytics, which enabled us to provide assurance over the completeness, validity and integrity of the payroll, and the quality of data, over the 12 months sampled.

6.1

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 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. There are still controls to be refined and issues to be addressed but there are agreed actions to ensure these are covered off.

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



Sponsor:
Mo Kang

Audit findings:

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.

POL00423508

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



Sponsor:
Rob Houghton

Audit findings:

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. 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:

- SPO's mandate is not clear and does not drive the implementation of delivery processes and the incremental improvements.
- SPO should agree with GE the sanctions for not delivering in accordance with the revised framework.
- Unclear roles of the Design Authority (DA), Enterprise Architecture Group (EAG) and the Change Approvals Group (CAG).

While finalising this review, we were made aware of imminent governance changes driven by the McKinsey report, which will further enhance change delivery in Post Office.

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.

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



Sponsor:
Rob Houghton

Audit findings:

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.

6.1

POL00423508

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



Needs Improvement

Sponsor:
Debbie Smith

Audit findings:

P1	1
P2	6
P3	0
Total	7

The shortcomings noted by 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.

Post-acquisition: Shortcomings in the Day 1-100 plan (being throughout the first 100 days only a subset of all transition activities), combined with insufficient resource planning, and 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.

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.

6.1

POL00423508

POST OFFICE LIMITED
AUDIT RISK & COMPLIANCE COMMITTEE

Cash Management System Upgrade - review

Author: Benjamin Cooke, Russell Hancock **Sponsor:** Rob Houghton **Meeting date:** 29th July

Executive Summary

Context

Transtrack 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, IRRELEVANT

IRRELEVANT

The Transtrack CWC 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 Transtrack's architecture and delivery capability. This paper outlines the residual risks with Transtrack, the steps management are taking to mitigate operational, financial or branch risk and our recommendation for Transtrack's future at the Post Office.

7

Questions addressed in this report

1. Who are Transtrack 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

- Transtrack is a critical application for Post Office supporting our Supply Chain cash and logistics capability. The Supply Chain teams' efficiency using Transtrak is improving as they become more familiar with the application.
- Our auditors have signed off the 2018/19 accounts including the Transtrack reconciliation gap on the evidence provided. Our reconciliation issues are now significantly reduced with the team continuing to make progress in fixing route causes.
- Operational teams are ensuring that our financials are robust and on-going controls are being put in place track down the remaining issues, and ensure that should similar issues occur in future, they would be quickly spotted.

POL00423508

- Transtrack have signed up to an improvement plan following our architectural review. They remain a close and committed partner and have invested significantly to overcome the application challenges. Provided this continues through to resolution we expect Transtrack CWC to remain a core application of the Post Office for some time, and are not adverse to investing further in the platform – taking care with commercial model and technical approach.

The Report

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

1. Transtrack are a small software company focused entirely on currency logistics and management technology, recently acquired by G+D a larger Germany firm who primarily sell currency machinery, and provide Post Office's Bank of England approved high speed note counters.
2. Post Office first procured Transtrack's 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.
3. Since POLSAP was designed out of Post Office's application landscape on February 2019 Post Office's entire Supply Chain cash processing and logistics has operated entirely using Transtrack's applications. A timeline of key events is provided in the appendix.

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

4. The key risks being monitored relating to Transtrack CWC 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 Transtrack not always being sent to our financial system.		**5**	**4**

POL00423508

Risk Title	Likelihood	Impact
Description	**Mitigating Action**	
Since February 2019 the CWC 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 35k transactions. The project team and Transtrack have 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 understated 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 absolutely ensure no impact to Post masters or financials.	• Post Office's auditors have now signed off 2018/19 accounts including the Transtrack reconciliation imbalance based on the evidence provided. • Technical progress is being made on solving this issue after Go-Live around 5% of transactions were missing every day, this figure is now 0.2% (around 20 transactions). • Supply Chain conduct physical cash counts weekly to ensure actual cash matches CWC 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 cleared the bulk of the 35k with around 6k 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 Transtrack's 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, Transtrack CWC 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 Transtrack application failures, and Transtrack are unable to quickly diagnose and fix due to issues with Transtrack's application architecture and delivery capability		**2**	**4**
Challenges through back office transformation have exposed flaws in the Transtrack application architecture, their development capacity, deployment approach and skills. There is a risk of future service disruption, IRRELEVANT **IRRELEVANT**	• 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 Transtrack and been resolved quickly by the support team. • Accenture technical specialists have been engaged to conduct an architectural review. Transtrack 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		

POL00423508

Risk Title		Likelihood	Impact
Description	**Mitigating Action**		
It is also worth noting that Transtrack have just been acquired by G+D 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 G+D and Transtrack leadership through the process.		**2**	**3**

What is the future for Transtrack in the Post Office?

5. The cost and complexity of migrating to a new Supply Chain system is high. Whilst project delays have been frustrating Supply Chain the application is now implemented, processes well understood and broadly performing well.
6. Inbound processing at our Supply Chain depot in Belfast – the first to Go-Live on Transtrack CWC – 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.
7. There are some scenarios in which Post Office may wish to integrate additional systems or invest in further Transtrack functionality. Our view is that this is still a viable option provided that the right approach is taken to the commercial framework used with Transtrack, and that any project is set up to maximise their strength taking account of their capacity and quality issues.
8. Transtrack 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.

Strictly Confidential

POL00423508

Appendix

Timeline of Events: Transtrack

Year	Event	Description
2005	Post Office Transtrack CViT bought	Post Office tenders for a CViT application for Supply Chain and Transtrack wins
2015	Post Office IT moves to a SIAM tower model	Transtrack is defined as a back office application. Accenture wins Back Office tower hence Transtrack is planned to novate Transtrack into the Accenture Back Office Tower.
2016	Transtrack CViT Upgrade	In June a project goes live upgrading Transtrack 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	Transtrack is paused from on-boarding to the Accenture back office tower	In August a decision was taken not to migrate Transtrack and novate to Accenture as: IRRELEVANT
2017	Decision taken to migrate POLSAP Cash Processing functionality to Transtrack CWC	In early 2017 the Back Office Transformation program team and Supply Chain recommended migrating from POLSAP onto Transtracks CWC module, purpose built for Cash Processing.
2017	Decision taken to custom build additional forecasting functionality in Transtrack (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 Transtrack.
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

7

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

1. This paper focuses on the two more recent decision points, firstly the decision to select Transtrack CWC 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.

POL00423508

Cash Processing Application

2. 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 IRRELEVANT 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 system, migrating to Transtrack CWC or starting a 3rd party application procurement.
3. *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.
4. *Transtrack CWC* – Transtrack invested a couple of months to create a "quick scan report" reviewing how closely Supply Chain processes fit to the Transtrack CWC application. The project created a "CWC High Level System Assessment" and visited two Transtrack CWC client sites to see the system in operation.
5. *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.
6. The team report a decision was made to select Transtrack CWC in a Steering Committee or Project Delivery Group meeting, however whist a decision document was drafted and requirement gathering began with Transtrack, it isn't recorded formally in any meeting.
7. There were a number of lessons learned on technical due diligence, partner management and governance.
8. *Technical Due Diligence* - Post Office's largest cash counting sites are 5x larger than Transtrack's next largest customer. Whilst the Cash in Transit (CiT) application had been performing at Post Office scale for some time the application architecture of CWC 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.
9. *Working with smaller partners* – Transtrack's 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

POL00423508

more thoroughly and B) in the case of issues talent can be re-prioritised by management to assist. IRRELEVANT

IRRELEVANT

IRRELEVANT 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.

10. *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

11. Having evaluated the basic forecasting capability within Transtrack CWC it was clear that additional features were required, yet Post Office's requirements were relatively basic compared to most retailers. Two options were considered:

IRRELEVANT

12. Post Office worked with a specialist supply chain consulting firm to evaluate options and get to a recommendation that the Supply Chain team supported.
13. The decision was recommended by the Cash Processing Project Delivery Group (PDG) then approved at Steering Committee.
14. 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.
15. It should be noted that PO instructed Transtrack 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.
16. Since go-live forecasting has been performed manually, with Power BI interim solutions going live in May.
17. The inventory management team have brought stock holdings down to levels prior to CWC migration successfully using manual forecasting. This is however labour intensive
18. An options paper is currently being written looking at options for the future of forecasting. IRRELEVANT being one of the options.

7

POL00423508

Belfast Datacentre Disaster Recovery Exercise

Author: Craig Bibby Sponsor: Rob Houghton Meeting date: 29th July 2019

Executive Summary

Context

The Fujitsu operated Belfast Datacentre hosts Horizon our Post Office counter trading application, and other business critical applications. The resilience of this datacentre has not been completely tested since 2013 due to the high risk of recovery of some obsolete applications (POLSAP) and equipment in the legacy estate. Post Office policy for critical infrastructure is to conduct annual IT Disaster Recovery (DR) tests to ensure that should an incident occur we can be confident of these plans. It is also a commitment to a number of our partners, clients and our customers. An exercise is scheduled for August Bank Holiday weekend 24th – 26th August 2019.

Questions addressed in this report

1. What does the Belfast Datacentre Failover Test mean for our Branches and our Business?
2. Which factors have been weighed when considering whether to proceed with this test?
3. What are our plans for the worst case scenario?
4. What are the risks of proceeding and how are they being mitigated?

Conclusion

1. We rely on the fact that Fujitsu's Belfast Datacentres would failover as planned in the event of a serious incident. As our key trading platform Horizon is critical to Post Offices trading. Whilst we believe in our plans, much has changed since 2013 and DR tests usually uncover wrinkles that require remediation to ensure smooth transition when in a real DR situation.
2. The Horizon system being unavailable is genuinely catastrophic to Post Office's ability to trade. There are contingency's for our most vulnerable customers that will provide some protection in the short term. Existing processes are in place to give emergency payments to POCA clients. Potentially any Post Masters who remained open to trade could direct bill payment customers to Payzone outlets, take some banking deposits or mails, reconciling back to Horizon when available. The vast majority of products and much of the network would likely close and not trade.
3. We have a high level of technical confidence that we can perform this exercise based on the previous successful DR test (2013) and regular component tests. A cross-discipline risk workshop has identified key risks, and mitigations have been identified where possible. Even if the test fails and we can't trade on secondary, we have a very high level of confidence in restoring primary as similar Horizon application shut downs occur monthly for patching.
4. In not performing this test we cannot be sure that our disaster recovery plans work. Having not tested this for 6 years breaks our obligations to our clients, and puts Post Masters and Clients at risk should something happen to our primary site. There are risks with performing the test and these have been mitigated and planned for as best possible. There is some risk of a short outage, and being our core trading platform any impact to Horizon essentially stops Post Office Network trading. On balance we believe it is right to proceed accepting this, but improving our overall business risk position.

Input Sought

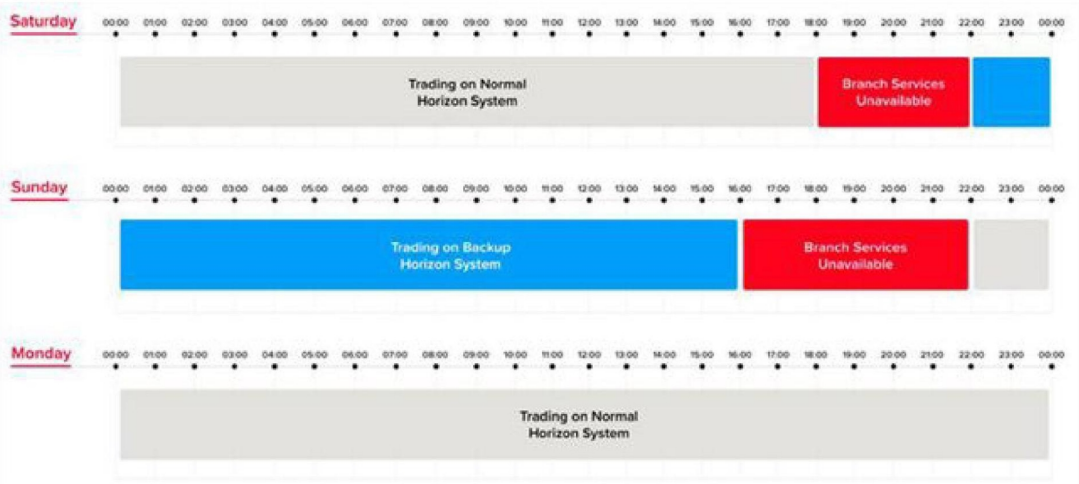
None

POL00423508

The Report

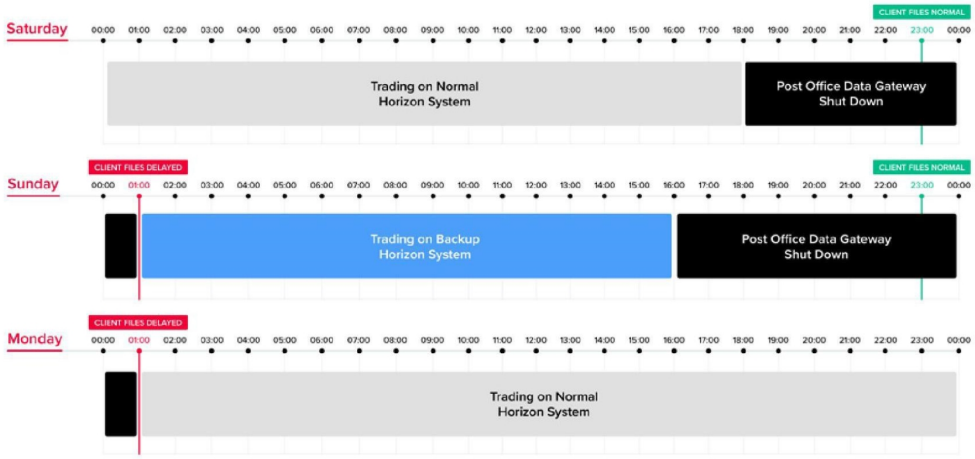
What does the Belfast Datacentre Failover Test mean for our Branches and our Business?

5. The Belfast Datacentre hosts Horizon, the trading platform used in all our branches and our critical financial settlement systems. During the failover the applications will shut down entirely as we switch from primary to the secondary ("backup") version in another datacentre.
6. The failover test is planned to be conducted within a weekend, with all technical activity conducted outside of core business trading hours. On Saturday night we will switch from normal trading on the primary Horizon system, to trading on our backup. All day Sunday businesses will trade as normal, noticing no difference, on secondary. Sunday night we will switch back to primary. This should complete by 10pm on Sunday, ready for Monday trading as usual.



7. The plan contains contingency time, and a bank-holiday weekend has been selected as trading is usually considerably lower. In the case of any issues over the weekend, the impact to trading would be reduced. Last August bank holiday saw an 88.3% reduction in transactions compared to an average Monday's trading, this includes data from the 1507 Scottish Branches for whom this is not a bank holiday.
8. The other major application to be shut down is our primary legacy integration platform (Post Office Data Gateway, PODG). This moves files to and from our Partners (e.g. banking, bill payments), and Back Office Applications. The impact of file delays will be mitigated by giving advanced notice of file delays and working with clients and suppliers to mitigate any impact to customers. This is done through the Post Office client relationship managers on an individual basis. The overnight file batch for back office applications will be mitigated with no planned impact to customers. These files will be delayed by approximately two hours and Accenture will provide additional support during the exercise so that files are processed with no impact to customers.

POL00423508



Which factors have been weighed when considering whether to proceed with this test?

9. A full Belfast Datacentre failover has not been possible for a number of years but with POLSAP decommissioned is now possible. In weighing whether to proceed we have considered the items below.

8

Factor	Considerations
The risk to Post Office trading from an inability to successfully failover in a disaster situation.	➢ Horizon is a resilient application and it is unlikely it would require an entire datacentre failover, but certainly a possibility, and one that could be triggered by physical or network events outside of Fujitsu's control as well as systems or process failures. ➢ The last successful test was 6 years ago, since which there has been considerable change. ➢ A number of component tests have been completed over the years, including a relatively recent complete database failover for Horizon. ➢ Having not completed a full test DR for 6 years when our policy is annual, we cannot say that we have high confidence of success should a disaster occur. Experience with DR tests of this nature indicate that challenges will be found in the process that can be resolved in a safe environment to prevent delays or failure should DR be invoked for real.

POL00423508

Factor	Considerations
How long Post Office bears the above risk	➢ In this year's change prioritisation the Belfast Datacentre exit was delayed. Current plans indicate that the application will not complete migration until June 2021, a further two years. ➢ Whilst core elements could be planned to be brought forward, equally decisions could be made to maintain the status quo for considerably longer. Whilst this remains unknown it is prudent to plan for Belfast Datacentre to remain critical for Horizon for 2-4 years.
Commitment to clients	➢ In Post Office's client contracts we commit to annual DR ➢ In the Banking Framework Post Office commits to annual DR for key systems.
Group litigation and media coverage	➢ This test was originally scheduled for May 2019, this was postponed due to the Horizon trial. The results of which will be published in mid-September 2019. ➢ Communications are being sent to the entire network to inform them of possible disruption and how to handle it. ➢ There is never a good time to conduct DR tests, but it's felt that with the Horizon Trial completed and the next bank holidays over Christmas or in May, this is a decent option.
The risk to the business of conducting the exercise	➢ Whilst standing up the secondary (DR) site has not been fully tested in 6 years. Shutting down and re-starting primary occurs monthly for patching. Hence whilst there is a risk that the test may not be successful, we are highly confident that we could re-start the Horizon primary system. Checkpoints scheduled over the weekend ensure that a decision could be made to abandon the test, failing back to primary before opening hours. ➢ Should the business start to trade on secondary on Sunday and face serious issues, there would be up to 5 hours outage during trading hours, whilst the primary systems were restored. ➢ The risks of conducting the exercise are outlined in the 3rd section below.

What are our plans for the worst-case scenario?

10. The worst-case scenario is that Horizon cannot be brought back up in time for either the opening of the Scottish branches on Bank holiday Monday affecting the whole of Scotland, or the opening of the remainder of the UK on the following Tuesday. The longer into that week it takes to restore service the worse the impact will be. There have never been plans in place for the long-term complete failure of Horizon as a whole and it has never happened. Where individual branches have experienced a Horizon failure, they simply close for the time it takes to restore. The major impact of such a large scale failure will be for vulnerable customers and for those individuals and small businesses using the Post Office to bank money

POL00423508

which they would need to be able store securely on their own premises. All other services would stop. Encouraging branches to open would be a challenge, reconciliation post recovery would be difficult, and compliance would weaken trade by trade. The Board would have to accept risks in reconciliation across all branches and accept figures they are given manually.

11. As stated above there is no existing plan for such an eventuality – it needs to be developed. Our approach should be to focus on two core products until Horizon comes back up:
    - POCA to support vulnerable customers – this is mitigated by manual payments made by Post Masters with later reconciliation to the system. This approach is in place but not well known and information and training would be required to ensure all branches were aware of the process.
    - Payments to support vulnerable customers – the strategy is to point customers to Payzone sites which would be unaffected by the Horizon outage. However in areas where the Post Office is the only outlet this may prove very difficult for vulnerable customers. Additionally currently Payzone bill payment contracts do not entirely overlap with Post Office, hence it's only a partial solution at best.
12. There is the option to support basic Mails products but this would be on a case by case basis at Postmaster discretion as most products would be difficult to support manually. All other products would be suspended.
13. If this test goes ahead then there would need to be a parallel plan of communications and preparation around the steps in 11 above. This would require significant effort and coordination using the Area Manager network.
14. The situation would need to be kept under close review requiring close coordination and communication with branches through the Area Manager network and Grapevine for outbound communications.

8

What are the risks of proceeding and how are they being mitigated?

15. A risk workshop took place on the 26th June with representatives from across the business. The session was to identify the business/operational risks associated with the failover exercise and to ensure the impacts are understood and mitigated as far as possible.
16. There is full risk register in place with mitigations and actions identified and a weekly review is in place to track progress. The current low probability, but high impact risks are shown in the table below:

Risk	Description
	Mitigation Plan
Branches are unable to trade on Monday 26th August (For Scottish Branches this is a normal working day)	➢ There is a risk that the 1507 branches in Scotland and other UK branches who plan to open, may be unable to trade at the time of opening on Monday the 26th August if the test does not complete on time. This would impact the ability to serve customers including trading for Scottish Banks which would result in reputational damage and financial impact to the Post Office

POL00423508

Risk	Description
Mitigation Plan	
➢ Data from last August for the entire network (inc. Scotland) shows an 88.3% reduction in trading when compared to an average Monday. ➢ Failover test to complete by 1am on the 26th August to allow for 6 hours of contingency if issues occur. The test plan will include regular Go-no calls to proceed to the next stage - Complete ➢ In event of exercise overrunning, the major incident management process will be implemented supported by invocation of the Business Protection team where required. - Complete ➢ Ensure communications are tailored to Scottish branches and Scottish banks. – In progress ➢ Fujitsu have upgraded legacy hardware components (bladeframes) to a higher calibre component which improves the service recovery time. - Complete ➢ Powerdown of application takes place on a monthly basis – Complete ➢ Communications to branches will continue if Horizon is unavailable via agreed text blasts via Grapevine - Complete ➢ Ensure manual business continuity processes are in place to provide POCA emergency payments to vulnerable customers. Customers are able to use ATM's to complete their withdrawals. Where we can, payments can be made at our Payzone locations. - Complete. ➢ Ensure correct stationary is in place across the branch network and issue refresher guides to the branches on "how to" . – In progress	
Horizon cannot be restored in either datacentre for a longer period.	There is a risk that Horizon cannot be restored in either datacentre. This would impact our ability to serve customers in branch, loss of remuneration but also reputational and breach of third-party obligations and potential fines (RMG/Banking Framework partners) resulting in financial and reputational damage.
➢ Mitigations as per above risk impacting over a wider scale.	
Decreased Resilience and data storage in secondary Datacentre	Should an issue arise with the main datacentre, Fujitsu are confident that we can continue to operate for some time on the second datacentre, however the levels of resiliency and data storage are reduced within the secondary datacentre as per design. Major items to note: ➢ There is no database replication outside of the secondary datacentre whilst operating when failed over. This means that should the entire database/datacentre fail – the days transactions would be lost. ➢ There is only a single branch network link into the secondary datacentre. If this fails for any reason, Horizon would be inaccessible.

8

POL00423508

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.

9.1

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.

POL00423508

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.

POL00423508

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

POL00423508

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

POL00423508

Business Continuity Risk Appetite

9.2

Author Tim Armit
Date June 2019
Version 0.1

POL00423508

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

POL00423508

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

POL00423508

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					

POL00423508

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. We are confident all systems will prove to be resilient and as test results are received the red will be removed.

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. Verizon runs across two datacentres UK5 and UK4 and the mutual support between these has not been tested. It was postponed in 2018 as there wasn't enough information on the impact on the connection between branches and Fujitsu's IRE11 and the ability of the Fujitsu datacentre to manage the load of the reconnections (that has since been tested and confirmed). Testing of the UK5/UK4 resilience is scheduled for the month of September 2019.	Red
Call Centre ACD/IVR	Averse	Loss of ability to manage calls to NBSC	2 hour recovery time	Puzzel which manages the Call Centre incoming calls, does not fall directly under Post Office control and its levels of resilience are being investigated. Status up date in September .	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. Status up date in September .	Red

POL00423508

Systems	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
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. Test scheduled for August Bank Holiday weekend.	Red
APOP	Neutral	Loss of payments out system	Recovery within 2 working days	The system remains a stand alone PC in Chesterfield. Status up date in September when this is planned to be relocated.	Red

POL00423508

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. It is not expected that any suppliers will not have proven strategies in place and we are confident the red will soon be removed. 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	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	Amber / Red
Computacenter	Averse	Unable to deliver system support to Post Office systems	Zero down time	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	Amber / Red
ATOS	Averse	Unable to deliver system support to Post Office systems	Zero down time	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	Amber / Red
Accenture	Averse	Unable to deliver system support to Post Office systems	Zero down time	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	Amber / Red
Ingenico	Averse	Unable to process card payments	2 hour recovery time	IRRELEVANT Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	Amber / Red

POL00423508

Suppliers	Appetite	Risk	Requirement	Contingency Strategies in place	Strategy Status
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 with an update in September.	Red
CBRE	Averse	Unable to respond to building issues	Intra day recovery times	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	TBC
Servest	Averse	Unable to support the management of key locations	Intra day recovery times	Letters sent to the supplier asking them to confirm their continuity capability and tests to prove this. Status up date in September .	TBC
Banks	Neutral	Unable to deliver support to operations externally to support the Banking Framework	Intra day recovery times	Post Office contracts with Banks do not state they have to demonstrate their continuity capability or report they test this. Post Office relies on the Banks to process incoming cheques and confirm incoming and outgoing monies. They also process the incoming cheques. If they were not available for 2 days branches would continue to serve customers but Post Office finance operations and confidence would weaken over time. It is expected that all Banks will have strong proven business continuity plans in place to meet their own and Regulatory needs, as such this is assumed to be a low risk. However at this stage Post Office has not had sight of these plans. Work in underway with the Banking Framework team to determine how to capture this information.	Amber / Red

POL00423508

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 IRRELEVANT 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	IRRELEVANT solution in place and tested	Green
Bristol	Averse	Loss of cash ordering process	Recovery Office	IRRELEVANT 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 IRRELEVANT solution in place.	Green / Amber
Bolton	Tolerant	Loss of internal human resources support services	Recovery Office	IRRELEVANT solution in place and tested	Green

POL00423508

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 September. 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

POL00423508

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	IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT solution in place for meetings to support home working.	Green
Finance Service Centre	Neutral	Unable to make payments or reconcile incoming monies	IRRELEVANT 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	IRRELEVANT 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

POL00423508

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 IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT solution in place for meetings to support home working.	Green

POL00423508

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 IRRELEVANT for the provision of office space to meet business needs. IT link to the IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT solution in place for meetings to support home working.	Green
Bolton HRSC	Tolerant	Unable to respond to internal HR queries	IRRELEVANT 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 IRRELEVANT 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 IRRELEVANT solution in place for meetings to support home working.	Green

POL00423508

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

POL00423508

[*GROUP POLICY*]

[*Business Continuity Management*]

9.3

Version – V2.4

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

POL00423508

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

9.3

POL00423508

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.

POL00423508

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.

POL00423508

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

POL00423508

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

POL00423508

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.

POL00423508

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

POL00423508

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.

Post Office Limited - Audit Risk & Compliance Committee-29/07/19

POL00423508

Post Office Limited - Audit Risk & Compliance Committee-29/07/19

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

POL00423508

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 - Audit Risk & Compliance Committee-29/07/19

POL00423508

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.

POL00423508

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;

POL00423508

- 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.

POL00423508

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).

POL00423508

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: 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.

9.3

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: GRO

POL00423508

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.

POL00423508

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*

9.3

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.

POL00423508

Strategic Portfolio Office (SPO) and Change Excellence Overview

Author: Tim White Sponsor: Rob Houghton Meeting date: 29 July 2019

Executive Summary

Context

At the ARC meeting in May, there was a discussion around Change risk and how learnings should be taken on board. The Chair requested that at the next ARC meeting an overview of the Strategic Portfolio Office (SPO), the Change Delivery function and the supporting governance structures is presented. In the past 12 months the Change Excellence programme has focused on improving the maturity of our Change capabilities (people, processes, governance, tools, data and metrics) from level 1[1] to level 3.

In April 2019 the GE approved to transform the way we deliver Change by creating 9 new portfolios, comprising all BAU, GLO and Blueprint initiatives, reporting directly in to a new Chief Transformation Office reporting directly to the CEO. The objective for this transformation is to bring the systems of management and delivery much closer together thereby improving visibility and control, simplifying governance, speeding up decision making, minimising silo'd working and reducing costs. This new approach also allows us to more effectively embed and enforce the new capabilities created by the Change Excellence programme.

In May 2019 Internal Audit reviewed the status of the programme and acknowledged that significant progress has been made towards this goal and that the programme had laid the foundations to drive a step change in change capability within Post Office but stated that the impact of these enhanced capabilities was dependent on the extent to which they are effectively embedded.

10

Questions addressed in this report

- How does the SPO/Post Office manage change
- What governance structure and controls are in place

[1] Level 1 maturity = processes poorly defined and controlled, outcomes unpredictable, and Change function is reactive. Level 3 maturity = processes defined and adhered to, outcomes increasingly predictable and Change function is proactive.

Strictly Confidential

POL00423508

Conclusion

1. The SPO, reporting in to the Chief Transformation Officer (CTO), governs all change across the Post Office with support from central Risk and Assurance (CRA) and Internal Audit. The 19/20 Change book of work which includes all Change initiatives pertaining to BAU, GLO and Blueprint is delivered by nine Portfolios covering 153 active projects with a 2019/20 budget of IRRELEVANT Each portfolio has a GE -1 sponsor and a portfolio director who reports directly in to the CTO and is accountable for delivering the overall strategic outcomes of the portfolio within the agreed budget and timescales. In this new structure all Change personnel including programme and project managers now directly report in to the portfolio directors and ultimately the CTO thereby giving the CTO and SPO the control to embed the enhanced Change capabilities.

2. Within the 19/20 Change plan, IRRELEVANT has been allocated to delivering operational improvements relating to GLO whilst a further IRRELEVANT of opex spend will be used to improve the relationship with agents. This IRRELEVANT of investment has already been identified of which IRRELEVANT has been committed to date. The end to end 'agent lifecycle' and associated signature policies and processes have been impact assessed against the Common Issues Trial Judgment with the necessary changes to ensure 'compliance' either already made or in train. These changes and progress of these initiatives and their specific and measurable business outcomes will be tracked and reported on at each Board. Pre-established governance (e.g. Board Sub-Committee meetings) and regular briefings / exceptional meetings gives the Board visibility of legal developments and these will continue. Further, as operational improvements are fully 'stood up' with projects mobilised, they will follow the Change Excellence Framework with their own respective programme teams adhering to the required level of governance.

3. The Change Excellence Framework has been developed as part of the Change Excellence programme and is being embedded by the SPO to support the management and delivery of change. It provides key documents, governance structures and guidelines which are continually improved and embedded throughout the Group.

4. Corporate governance structures with delegated authority have been established by the SPO to manage change, taking into account the scale, complexity and the level of investment funding required. The Design Authority and Change Approval Group (CAG) have been merged and re-purposed. The PRB members are now all GE -1 with a broad cross-business range of experience thereby ensuring better more informed investment decisions.

10

Input Sought

This update is for information only as requested by the ARC. No input is sought.

Strictly Confidential

POL00423508

The Report

How does the SPO manage change?

1. As a commercial business with a social purpose our strategy requires us to balance the goals of continuing to provide essential services to our customers with the need to significantly and continuously grow our profitability over future years so that we can continue to reinvest in our business and communities. Successfully achieving this strategy whilst maximising returns on investment within acceptable risk tolerances requires a mature, agile and integrated Change capability.

2. The Strategic Portfolio Office (SPO) vision for Change Excellence incorporates 'doing the right things' and 'doing things right' with a focus on understanding the value of initiatives, increasing the speed to value and decreasing the cost to value.

3. In November 2017, the Group Executive (GE) endorsed a proposal which concluded that due to a number of systemic problems the current Change capability was not mature enough to deliver the strategic outcomes of the business and recommended that changes to structure, governance, culture and competency so as to address these fundamental issues. As a result the Change Excellence Programme was established.

4. Throughout 2018/19, the SPO has made progress towards target outcomes for the way that the Post Office manages change through the Change Excellence Programme, this being reflected in an increase in our Change Capability Maturity from a score of 1 at outset to 1.9 in October 2018 to 2.5 at the end of April 2019 and forecast 3.5 once fully embedded. The outcomes delivered to date include:
   - building a system to create a single source of truth for all projects in ServiceNow (current features include status, financials, lifecycle stage, risks, issues. Further improvements continue to be implemented along with validation of all data held in ServiceNow);
   - continued reconciliation between ServiceNow, SAP and Anaplan to resolve discrepancies in financial figures, providing increased understanding of and a firmer basis for financial control;
   - defining a lifecycle and associated artefacts and processes for both waterfall, agile and hybrid initiatives;
   - implementation of improved senior management and UKGI reporting;
   - establishment of a Competencies framework for all change roles;
   - introduction of binding principles and critical success factors as mandatory gating rules;
   - the design of a benefit management system and supporting leading indicator dashboards;
   - implementation of a revised Assurance process; and
   - improving the utilisation of more Agile and effective ways of working, by adopting the standards of the Scaled Agile Framework (SAFe), on-going training of the Change and wider Business community, coaching for specific projects and individuals, and support on appropriate organisation structures, roles and responsibilities.

Strictly Confidential

POL00423508

5. In addition, nine new change portfolios have been established and GE is now collectively accountable for their overall performance. Each is led by a Portfolio Sponsor and Director, who together are accountable and responsible for delivering the Vision, Outcomes and Financial objectives of their portfolio. These new portfolios have replaced the existing Business Unit ones with three exceptions: Peregrine, Telco and Insurance. These new Portfolios will:
   - bring the systems of management and work closer together to speed up time to value;
   - provide more focus on achieving strategic outcomes and building signature processes;
   - ensure the GE is collectively accountable for the success of all portfolios;
   - address our fragmented capability issue;
   - encourage cross-business unit working;
   - address silo'd thinking; and
   - reduce management overhead.

6. As a result of the revised portfolio structure and the strengthened clear lines of accountability, non-adherence to change standards and processes within the change delivery framework can thus be addressed directly via usual line management processes. The launch of the new structure has included communications to that effect, and job descriptions have been revised to further reinforce. Additionally, where hard controls can be applied, then systems and processes mandate adherence to such. Scheduled assurance, in the form of healthchecks undertaken by Change Risk Assurance, and ad-hoc reviews and support, undertaken by the Portfolio Directors, provide further opportunities to monitor. We continue to develop the information collected in ServiceNow to provide improved insight.

What governance structures and controls are in place?

7. The governance structure implemented by the SPO to manage change:
   - provides authority to proceed and progress the change initiative by having regard to strategic alignment, value for money and risk through the newly formed Project Review Board (PRB) and the Investment Committee;
   - identifies resource needs for each initiative and establishes an effective delivery team to ensure appropriate customer treatment, operational performance and management of risk;
   - monitors progress against the agreed deliverables, spend and benefits delivery including, as necessary, a review of the identification and management of key dependencies, issues and risks;
   - reviews, understands and approves any material changes to scope;
   - ensures all stakeholders are engaged and robust governance / decision making structure in place, and where appropriate a steering group led by the Accountable Executive. This includes appropriate oversight and control mechanisms and ensures appropriate recording keeping is undertaken for key decisions;
   - reviews and approves that the change is ready to go live considering the readiness of the business to accept the changes;
   - conducts formal project closure reviews;
   - identifies and shares lessons learnt; and
   - assures the subsequent delivery of benefits.

POL00423508

8. In addition to the above governance frameworks, the SPO works very closely with the Post Office Change Risk & Assurance (CRA) team (which sits within the Central Enterprise Risk function). The CRA leads on providing independent assurance of the overall change portfolio. Its primary stakeholders are the Director of Risk, The Director the Strategic Portfolio Office, individual Sponsors, business portfolio leads, programme//project managers as well as the Investment Committee and the Portfolio Review Board.

9. CRA provides a 2nd line change assurance function whereby the
   - 1st line: sits with individual programme/projects. They own their change risks and are responsible for managing them and assuring effective change delivery
   - 2nd Line: sits with the CRA (along with the SPO itself). The CRA provides assurance on change risks and compliance with corporate standards. In effect CRA oversees the change risks and provides assurance of the 1st line.
   - 3rd Line: is Internal Audit which provides full independent assurance of change risks. It assesses the effectiveness of change governance, change risk management, including effectiveness of 1st and 2nd Line and reports directly to ARC.

10. The CRA provide a number of formal outputs including
    - Pre-Business Case assessments: an Independent assessment of a programme/project during the Prove phase and before they seek approval of their Business case. It assesses where the programme/project is set-up to succeed, there is a good strategic fit, clarity is provided on the main stakeholders, scope is understood, realistic plans are in place and the main risks have been identified. It also assesses where the programme/project is affordable, achievable and will deliver VfM.
    - Health checks: again an independent assessment of a programme/project but after initial funding approval. It assesses delivery confidence across time, costs and benefits. It also looks at the stability of aims and scope, governance, risks & issue management and extent of business readiness. Recent Heath Check reports have been produced on GDPR, Horizon Integration Hub, Data Analytics, IAM (JML) and Fit & Proper.
    - Post-implementation Reviews (PIRs): an assessment post closure on whether a programme/project delivered its aims and objectives (within time, within cost and to the quality requirements (including the benefits). It compares final outcomes against what was laid down in the original (and any subsequently updated) approved Business Case. It looks at what went right (and why), what went wrong (and why) and what are the key learnings.

11. The various CRA activity has identified some common learnings across the various programme and projects that have been assured. This include the need to be tighter on what is and within scope at the outset and ensuring that material change to the baseline is formally changed controlled and approved by the relevant governance forum. We have also found evidence that scope creep can have a knock-on impact on the agreed timeline (which, on occasions, can slip) and the realisation of the associated benefits. The CRA team ensures such learnings are fed back into the SPO and help inform supportive change to the Change Excellence framework and process for example the design of a benefit management system and supporting leading indicator dashboards is a case in point

POL00423508

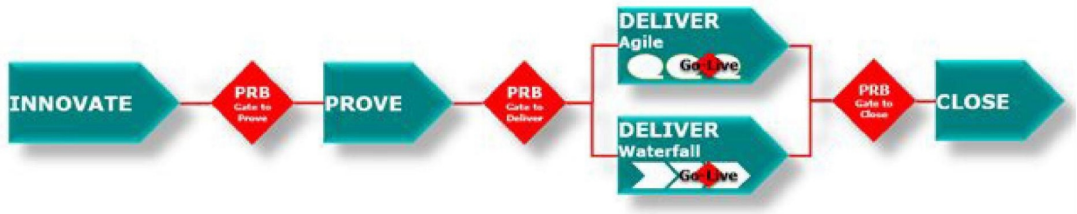
12. The CRA also undertake a series of regular reviews of programme/projects RAID logs (covering risks, assumptions, issues and dependencies). It assesses whether the information is complete, accurate, being proactively managed and up to date. These reports are provided to project managers and Business Portfolio Leads. Over the last 6 months we have undertaken about 60+ such reviews. We have found areas of good practice but some levels of full compliance with corporate standards is patchy. There is a tendency to focus on risks at the expense of assumptions, issues and dependencies and for the RAID to not always be the single version of the truth. The CRA are now looking to migrate change risk management to Service Now by August 2019 thereby putting in place a more efficient and effective capability and making compliance with corporate standards that much easier.

POL00423508

Appendix

1. Change Delivery Lifecycle / Framework
2. Purpose of the Investment Committee
3. Purpose of the Project Review Board
4. Governance Approvals
5. SPO Change Delivery Oversight
6. Mapping of new Portfolios
7. Change model maturity model

1. Change Delivery Lifecycle / Framework



2. Purpose of the Investment Committee *(taken from ToR)*

The purpose of the Investment Committee is to ensure that the investment provided by UKGI is used to deliver the agreed strategic objectives, as detailed within the North Star. As part of its scope, the Investment Committee will review demand and approve funding for new initiatives, approve changes to in-flight initiatives and also provide intervention \ support for resolution of any escalated issues. Its responsibilities and delegated authorities are as set out its terms of reference, changes to which must be approved by the Group Executive

3. Purpose of the Project Review Board *(taken from ToR)*

The Project Review Board (PRB) is a committee that has delegated authority from the Investment Committee to approve CapEx and Exceptional funding (within agreed limits), gate governance and quality assurance for projects. It is a decision making body.

10

4. Governance Approvals

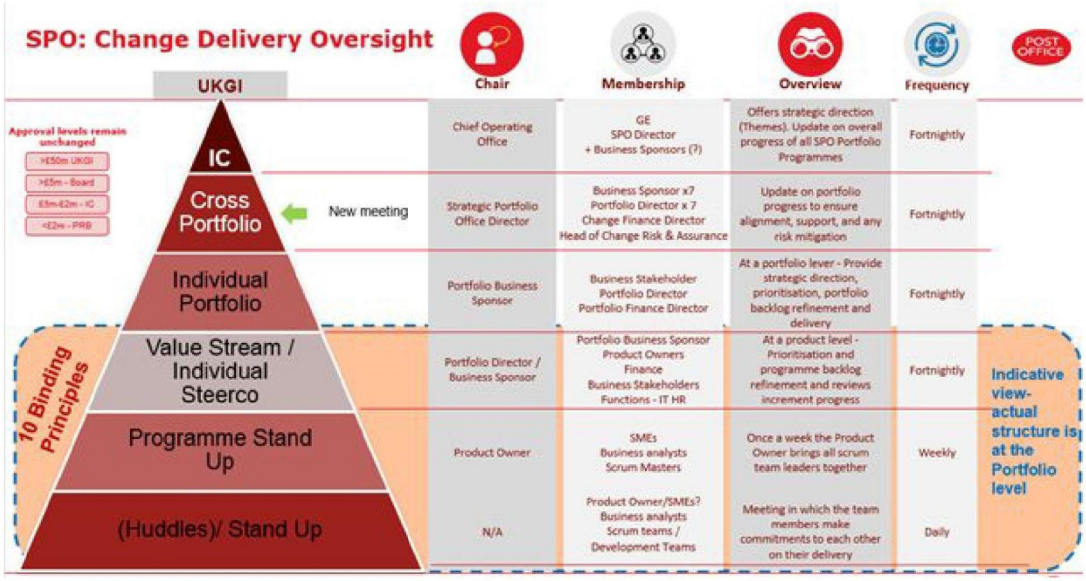
>£50m UKGI
>£5m - Board
£5m-£2m - IC
<£2m - PRB



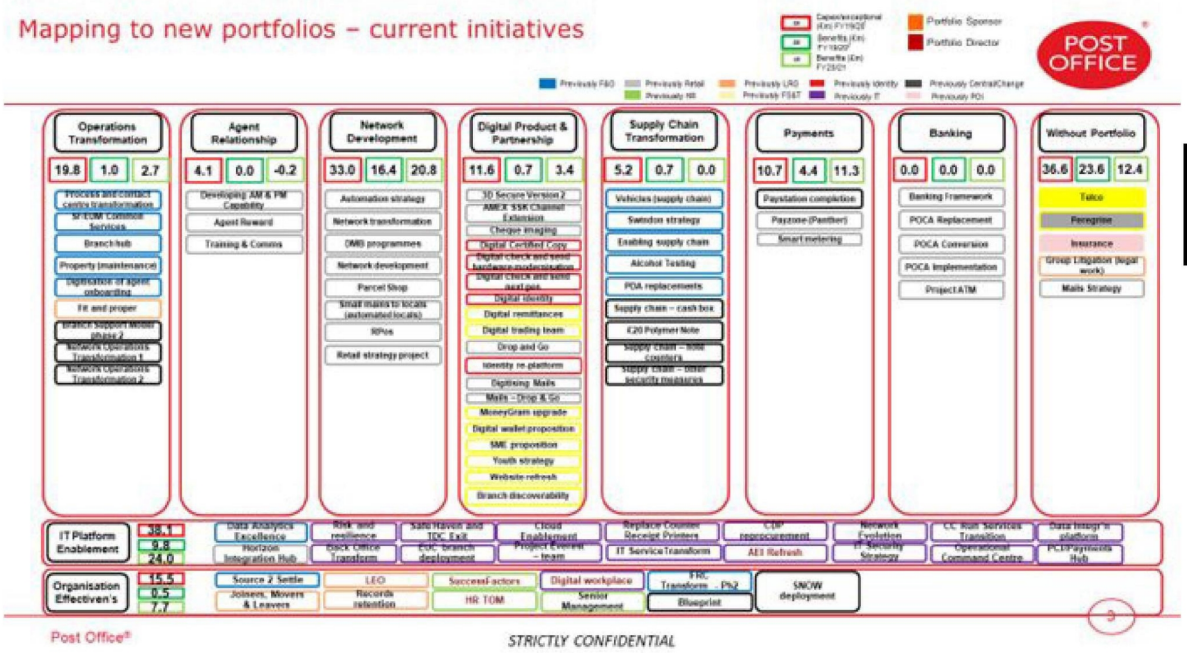
Strictly Confidential

POL00423508

5. SPO Change Delivery Oversight



6. Mapping of new Portfolios

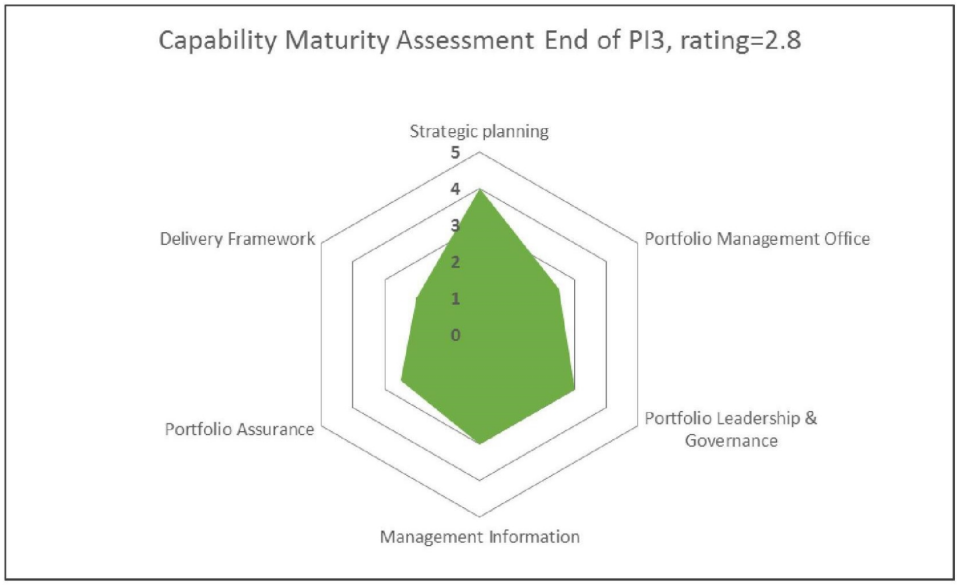


10

Strictly Confidential

POL00423508

7. Change Model Maturity Portfolio (end April 2019)



10

POL00423508

UK Data Protection Act (incorporating GDPR) Compliance Status Report

Author: Chris Russell Sponsor: Ben Foat Meeting date: 29th 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. In achieving effectiveness Post Office has high confidence that personal data can continue to be used to support our businesses. Substantive compliance was primarily focussed with evidencing that effectiveness could be maintained and demonstrated to both regulators and internal stakeholders.
- 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.

11

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?

[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*

POL00423508

- 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?

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. This allows regulators, key stakeholders and customer's confidence that Post Office can use the data it holds to support business operations.
2. There is still work to be done to implement further administrative controls that will enhance our ability to evidence that effective compliance has been achieved and maintained. In particular, separate projects in the following areas will help us achieve this:
    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".

11

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.

POL00423508

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

POL00423508

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

POL00423508

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 to end of August.

Conclusion

23. The overall compliance summary is that there has been significant improvement in Post Office's data protection processes, controls and culture.

24. 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 that deliver our business objectives

25. The remediation work identified in this paper needs to be completed to ensure Post Office can evidence that Risk Appetite for compliance with its legal and regulatory obligations are met. Enhanced internal Policies, Processes and Procedures will enable Post Office the ability to evidence this to regulators, key stakeholders and customers. (See the Annex below for high level information on Maturity Level of UK DPA18 compliance within Post Office.)

POL00423508

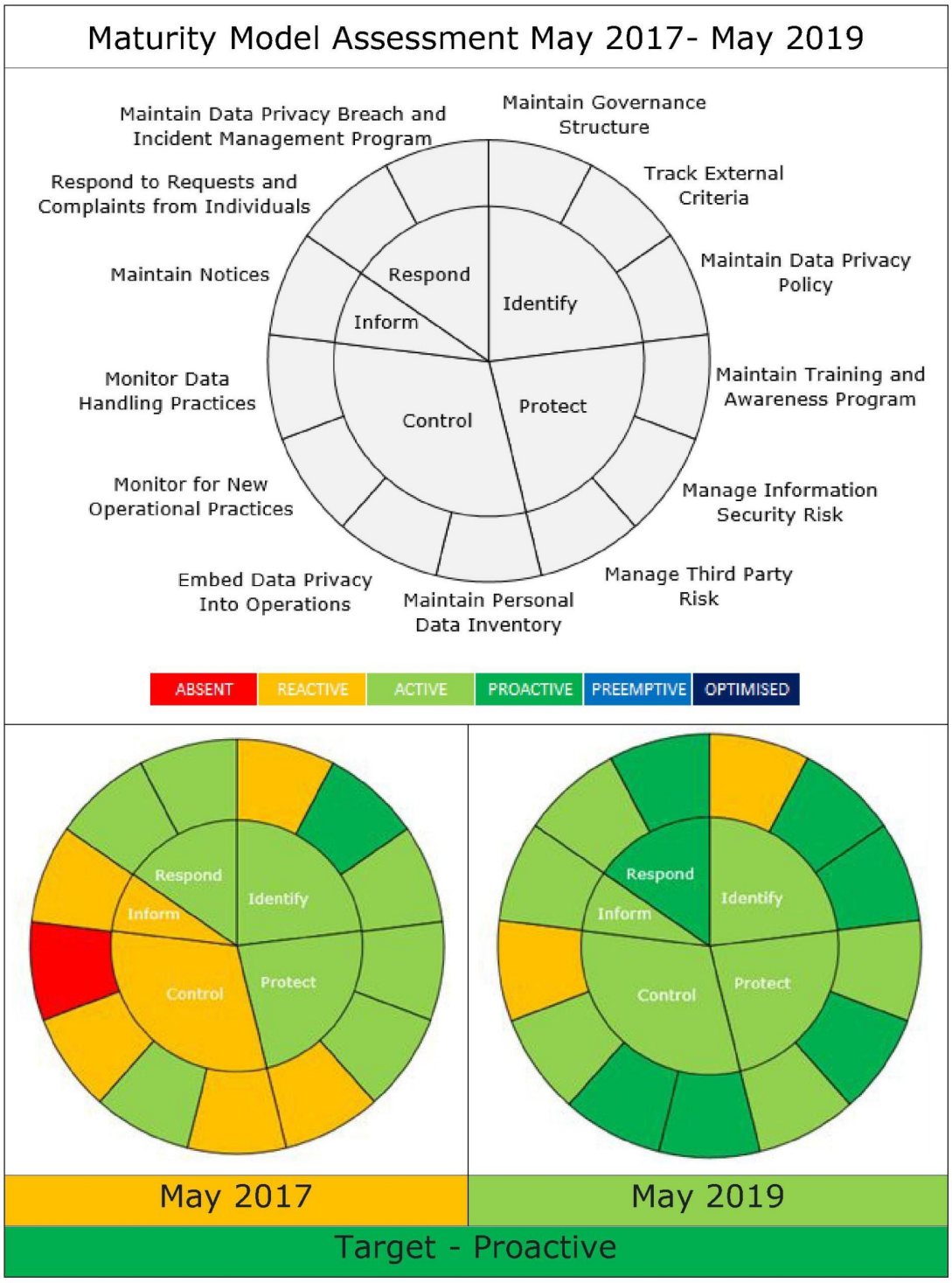
Appendix

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.

POL00423508



11

POL00423508

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.

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.

11