POL00004408

Fraud and Non-conformance in the Post Office; Challenges and Recommendations

G-119 Fraud Analysis

Detica NetReveal®

By J L Ferrari, S Coyle

1 October 2013

NRRA1207.10D007-0.50

51 pages including cover

Detica

BAE SYSTEMS

POL00004408

Version history

Version	Date	Author	Action
0.10	27 Aug 2013	SC	Outline draft
0.20	04 Sep 2013	SC	Full draft for initial review
0.30	17 Sept 2013	SC	Updates following internal review
0.40	18 Sept 2013	SC	Draft release for external review
0.5	27 September	SC	Iteration following review by the Post Office

Copyright statement

Document control

This section is optional and is used to describe any specific handling and deliverability requirements for the document and to whom the document has been distributed. This is usually only needed for a classified document.

POL00004408

1 Executive summary

1.1 Overview

Detica NetReveal has conducted a six month pilot study, referred to as the "Pilot", into the fraud and non-compliance issues faced by the Post Office. The Pilot evaluated the data available to security teams relating to branch activities and transactions and the quality of information and processes shared by central teams. The study also conducted a detailed data analysis of branch behaviour using transactional and branch metadata. Following these activities the Pilot has made recommendations into how the Post Office should address the issues highlighted.

The project has taken place against a backdrop of wide-ranging changes within the Post Office including the Network and Crown Transformation Programmes, reducing Government network subsidy, transformation of IT following Royal Mail Separation, launch of the Post Office Current Account, public discontent amongst Sub-Postmasters relating to the Horizon system, review of the Horizon system by Second Sight and strikes by Crown branch staff. Many of the issues encountered during this study underline the urgency with which the Post Office needs to adapt its business practices and technology to respond to these changes.

1.2 Key findings

The Pilot reviewed the policy, processes and information used by the Post Office to track and manage the compliance of branches. The short-comings identified within these areas pose serious risks to the financial performance of the business:

- The Post Office is unable to automatically check that stock sent to a branch has been sold nor the stock levels of each branch.
- The Post Office is not able to account fully for the whereabouts of significant values of cash in the network, particularly in the case of cash left in open transfers or moved to ATMs.
- The Post Office does not know how many branches are currently under suspicion, how many are a risk or how many have been passed fit by the security team.
- The Post Office is unable to quantify the financial impacts either direct losses or operational costs created by these risks.

We have identified four areas which contribute to these risks;

- Widespread non-conformance to Post Office policy and processes by branches, with an institutionalised acceptance that errors, workarounds and non-conformance exists;
- Complexity and fragmentation of information systems which hamper efforts both to gain an insight into branch behaviour and root causes;
- Ineffective process, policy and working practice in the central operational teams to gather information, prioritise and act in a co-ordinated manner;
- Technology available to central operational teams are not fit for purpose; analysis of large data sets is performed on an ad-hoc basis of data subsets copied into Excel and tasking of teams is initiated and managed through email.

POL00004408

1.3 Recommendations

We have made 39 recommendations, see section 7.3, as to how the Post Office should tackle the issues identified in the report. These are based on observations of the working practices of the Post Office, discussions with Post Office staff and experience of fraud operations teams in both the Public and Private sectors. Many of the issues identified by the report impact teams outside of Post Office Security as well as those inside. Similarly, many of the recommendations can only be implemented through sharing the burden and responsibility for change across the Post Office.

POL00004408

References

Mnemonic	Document Details	
[REF 01]	Title:	Post Office Fraud Solution Report
	Doc Ref:	NRRA1207.01 D001
	Version:	1.0
	Date:	18 May 2012

POL00004408

List of contents

1 Executive summary ... 3
1.1 Overview ... 3
1.2 Key findings ... 3
1.3 Recommendations ... 3

References ... 5

2 Fraud and Non-compliance pilot ... 7
2.1 Introduction ... 7
2.2 Findings from previous project ... 7
2.3 Project scope, approach and timeline ... 8

3 Business context and challenges ... 10
3.1 Approach ... 10
3.2 Business landscape ... 10
3.3 Business risks ... 11
3.4 Operating environment ... 13
3.5 Post Office Fraud Analysis security team ... 16

4 Post Office data sources ... 19
4.1 Difficulties extracting data ... 19
4.2 Alternative sources of data ... 19
4.3 Other important data sources ... 20
4.4 Data quality assessment ... 21

5 Data analysis – insight into branch behaviour ... 23
5.1 Observations on branch activity ... 23
5.2 Identifying high risk branches ... 25
5.3 Investigations into what causes branches to become risky ... 28

6 Case studies ... 35
6.1 Non-conformance ... 35
6.2 Ineffective training ... 35
6.3 Ineffective auditing of branches ... 35

7 Report conclusions and recommendations ... 37
7.1 Overview ... 37
7.2 Report conclusions ... 37
7.3 The case for change ... 38
7.4 Recommendations ... 39
7.5 Roadmap for the security team ... 43

A Data used in the Pilot ... 49
A.1 Data sources ... 49
A.2 Data quality assessment ... 49

B Key Risk indicators ... 52

C Branch list and risk ... 53

POL00004408

2 Fraud and Non-compliance pilot

2.1 Introduction

This report details the work undertaken by Detica NetReveal over a six-month period commencing in March 2013 into fraud and non-compliance in the Post Office branch network. The Pilot followed a previous study into the use of information by the Post Office security team [Ref 01] which identified a number of weaknesses degrading the teams' ability to adapt and respond to the challenges posed by the branch network. The purpose of the Pilot was t to investigate and demonstrate how Post Office security should change to meet these challenges.

2.1.1 Report Structure

The report is structured as follows:

- Chapter 2 (this chapter) outlines the background to the project, its scope, the principal activities and timeline.
- Chapter 3 describes the business context to the pilot, the teams involved in managing branches and the working practices of the Fraud Analysis team who are principally responsible for detecting and preventing financial loss.
- Chapter 4 evaluates the data quality of data sources made available during the study.
- Chapter 5 presents the results of our analytical studies on the behaviour of branches.
- Chapter 6 provides a set of case studies identified during the Pilot which highlight the challenges faced day-to-day in managing the branch network.
- Chapter 7 provides the key findings of the Pilot, recommendations on how the Post Office can improve and a road map for the security team.
- Appendix A describes the approach to risk scoring branches outlines.

2.2 Findings from previous project

The review into the use of information by Post Office security [REF 01] made a number of key observations regarding the factors hindering Post Office operations, including:

- Gaps in understanding of the Credence (transactions) database;
- Day-to-day operations reliant on bespoke (Excel spread sheets) databases;
- Unclear data ownership across the business;
- Fraud detection based on a short-term, summary data, rather than transactional level data over an appropriate time frame;
- Employee data for agency branches was reliant on Sub-Postmasters, 'SPMR's, and was difficult to access; and
- There is only a query based model for data access so only known problems can be verified.

The report made three recommendations:

POL00004408

- Consolidate data access: to reduce inefficiencies and duplication of data;
- Enhance available data: to enhance profiling ability;
- Automate fraud detection: to reduce manual interrogation and improve returns.

2.3 Project scope, approach and timeline

2.3.1 Scope

The Pilot started from the recommendations from the security review as the basis on which to conduct further investigation. The Pilot's goals were to:

- Understand where the Post Office loses money due to fraud and non-compliance;
- Develop fraud rules to identify unwarranted or risky branch activity;
- Demonstrate how the Post Office can extract more value from its data;
- Demonstrate how technology can be used to enhance team productivity;
- Develop a target operating model for the security team;
- Develop a roadmap to modernise the security team:
- Detail the return on investment or business case drivers for implementing a solution.

2.3.2 Approach

An agile methodology using monthly sprints was adopted to ensure the project could re-prioritise activities based on availability of data from target source systems and improved understanding of the exact scale and nature of operational losses impacting the Post Office. The project was organised into three complementary work streams; business analysis, data analysis and technology.

2.3.2.1 Business analysis

The business analysis work stream was tasked with documenting the current processes employed by the Post Office to detect losses, identifying the systems used and understanding the context in which losses occurred. Primary information gathering was undertaken through focus interviews with Post Office staff from teams identified to be involved with branch performance, support or supply. Where possible, evidence to support assertions made in these interviews, was sought by the team in the guise of data extracts, templates for processes, or management information.

The review evaluated the Post Office response with regard to:

- Business landscape; the wider changes to the Post Office beyond the Security teams which will impact how the Post Office operates;
- Business risks; known fraud risks and non-compliance issues posed by branches;
- Operating environment; the teams and processes used to detect and investigate suspected instances of fraud or non-conformance;
- Fraud Analysis team; processes, technology and data used by the Fraud Analysis team to detect and investigate branches.

POL00004408

2.3.2.2 Data analysis

The data analysis work stream was first tasked with identifying and evaluating data sources for use in the analysis of calculating the risk of each branch. The data sources were analysed with reference to ease of access and quality, including how well the data was understood by users, how up-to-date and how well it could be incorporated with associated data sources.

The second task was to use the data source to evaluate the behaviour of branches to identify unwarranted or risky behaviour. The team developed a set of Key Risk Indicators or "KRI"s, to model risky activity and then used these measures to develop a model to rank branch behaviour by their propensity to fail audits using historic records of passed and failed audits.

2.3.2.3 Technology development

The third work stream concentrated on configuring the NetReveal toolset to demonstrate how data and processes could be provided to the Fraud Analysis team to enhance productivity through greater insight into branch behaviour.

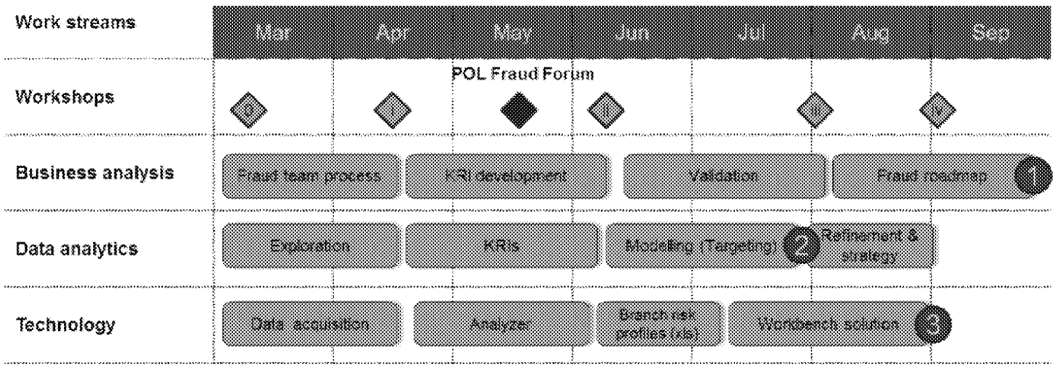
2.3.3 Timeline

The project committed to delivering three deliverables to be produced iteratively over the six month duration:

1. A project report including roadmap for Post Office security (this document);
2. A model to rank level of risk of each branch's behaviour;
3. A configuration of NetReveal toolsets:

    Workbench – to prioritise and record the investigation of branch behaviour

    Analyzer – to provide a central repository of important Post Office data sets previously interrogated in isolation from each other.



The project activities and their timelines are provided in Figure 2-1, below.

Figure 2-1: Pilot project timeline; numbers 1-3 denote approximate dates of delivery of deliverables described in 2.3.3; numbers 0-iv denote approximate dates of end of sprint workshops

POL00004408

3 Business context and challenges

3.1 Approach

3.2 Business landscape

The Post Office is unique in the number and variety of products and services it offers, the breadth and diversity of its branch network, and the geographical diversity of its central functions. These factors have strongly influenced the current Post Office response to manage fraud within the network.

The Post Office with the support of HMG is engaged in a series of wide-ranging and ambitious changes to make the branch network financially stable. Beyond the desire to reduce the exposure of the public purse is the recognition that the Post Office remains one of the few viable organisations to serve communities with the retrenchment of Government agencies and departments. The impacts are felt across its network and teams, exposing both new areas for fraud and non-conformance losses but also offering the opportunity to improve and enhance performance. Below we have reviewed the changes likely to impact the Post Office's exposure to fraud losses.

3.2.1 The Network Transformation programme

The Network Transformation Programme, ("NTP"), will change the way the Post Office does business, with modernised shop designs and layouts, different payment structures for SPMRs and extended opening hours.

The primary concern of the security team in the Post Office relating to NTP was the reduction in parachute payments for SPMRs. Financial stress has been identified as the main reason behind thefts by SPMRs; any reduction in payment by the Post Office without corresponding increase in retail revenues will likely increase the risks to the Post Office.

The adaptation of branches under NTP is costly; a branch shut for fraud soon after it has been remodelled represents a higher cost to the Post Office than normal and the risk of damage to the programme. There are some, so far un-corroborated, reports that this has led in a small number of cases to increased leniency.

3.2.2 The expansion of financial services products

The Post Office has a stated interest in expanding the range of financial services offered into retail banking and insurance sectors. These are highly competitive industries and well-established targets for fraudsters. Institutions in these sectors invest considerable sums in protecting them and their customers from increasingly sophisticated attacks. Typical controls in place involve tight control of staff activities, monitoring of customer interactions in real time, and social network analysis to identify customers with suspicious activities. In contrast, the existing fraud detection capability of the Post Office is far less well-developed; improvements in the security capability and preparedness will be a necessary step in the development of any additional financial services products.

Whilst the underlying product provider (e.g. Bank of Ireland) will be responsible for monitoring accounts for fraudulent purposes, without robust monitoring capabilities and near real-time communications between the Post Office and provider both organisations will struggle to detect if the Post Office is being used as the application point for the Post Office.

POL00004408

3.2.3 Second Sight

The initial findings of Second Sight were published during the Pilot. The review was prompted by a public campaign by SPMRs who felt they had been wrongly traduced by the Post Office following losses at their branches. Several of Second Sight's observations resonate strongly, notably the disjointed response by the Post Office and the habitual desire to assign responsibility to an individual rather than to conduct root cause analysis to close gaps persisting across the branch network. In order to have a consistent approach across the SPMR estate, it is vital that Post Office has the ability to robustly identify and monitor anomalous behaviour, so that the appropriate corrective action can be taken (whether this is tactical education, enhanced training, process or system re-design, or audit/investigation).

3.2.4 IT refresh

As part of separation from Royal Mail Group, the Post Office is relocating, and in some cases redesigning, a number of core systems. Of particular interest to the Pilot was the refresh of the Horizon hardware and application, given its importance as both a sales channel and a source of transactional data. The re-design offers the Post Office an important opportunity to rectify gaps which have previously exposed them to loss, and put in place a more robust monitoring process.

3.3 Business risks

The Post Office branch network presents a challenging picture for fraud detection and analysis. Throughout the Pilot, the assumption that activities should be performed in the same way as they have always been done has been prevalent. Despite this the Post Office has changed radically over the past 20 years, and in some cases the disconnect between current practice and what is required is striking. As made clear in this report the Post Office cannot adequately tackle fraud until the scale of the Post Office non-conformance problem is reduced.

3.3.1 High levels of non-conformance

Within the branch network, business practices are known to differ between branches. Whether through lack of knowledge, poor system design, or wilful disinterest in compliance, a significant number of SPMRs do not comply with official business practice.

Examples raised during the Pilot include:

- Not declaring cash on hand accurately or at all, or before the close of business. The cash management team use this figure to generate part of their cash delivery to the branch network, therefore declarations that are missing or at a drastically different time, can result in an inappropriate cash flow to the branch.
- Declaring a '16:30' ATM balance, at a time other than 16:30 will affect the branch balance and create errors and the inability to defend fraudulent retract transactions.
- Cash kept in open transfers overnight; especially prevalent in Crown branches. Currently cash management do not have open transfers included in their cash holding figure, It is thought Crowns keep cash in open transfers overnight to meet their 'target holdings', This pilot calculated that on average £900,000 was kept in open transfers overnight, representing a cost of approximately £30,000 a year.
- Activating all scratch card packs when new stock received
- Selling non-Post Office products through the Post Office till. Many Post Offices offer 3rd party products for sale; which should not be sold through the Post Office till. In

POL00004408

practice SPMRs will usually sell the item as 'Postage other' then reverse the transaction at the end of the day. Furthermore, if these purchases use debit or credit cards the Post Office bears the additional acquiring charges to process the transaction without any remuneration. In addition to the financial loss, the Post Office is also in breach of its contract with its acquirer as this allows the processing only of transactions relating to Post Office business.

The widespread instances of non-conformance expose both the Post Office and SPMRs to the risk of financial loss. Instances of non-conformance also generate operational noise which hides deliberate attempts to defraud it. This has resulted in a large number of false positives when looking for fraud, and inhibits Post Office's ability to detect fraud early, resulting in larger losses. For the SPMR, the risks are that poor practice will lead to a failed audit, theft by employees or indeed increased temptation.

3.3.2 Insecure systems and processes

A number of systems have been designed without sufficient attention paid to the security implications. This has produced gaps through which poor practice, non-conformant or fraudulent behaviour has arisen. Below we provide several of the most important cases identified.

3.3.2.1 Stock management and reconciliation

There is a currently no central reconciliation between the stock ordering system, Galaxy, and Horizon with stock delivered to a store manually entered into the Horizon system. Figure 3-1 illustrates how the lack of reconciliation or verification could be exploited to hide losses. A stock order by a branch is not automatically checked to confirm the branch requires stock, nor that when dispatched the stock is correctly accounted for in the Horizon system.

A branch experiencing a shortfall can cover the shortfall either through not entering the stock in Horizon and selling it outside of the system or adjusting the stock. Stock adjusting upwards reduces the cash required to balance the branch and subsequent false over claims of returned stock can bring branch snapshot right.

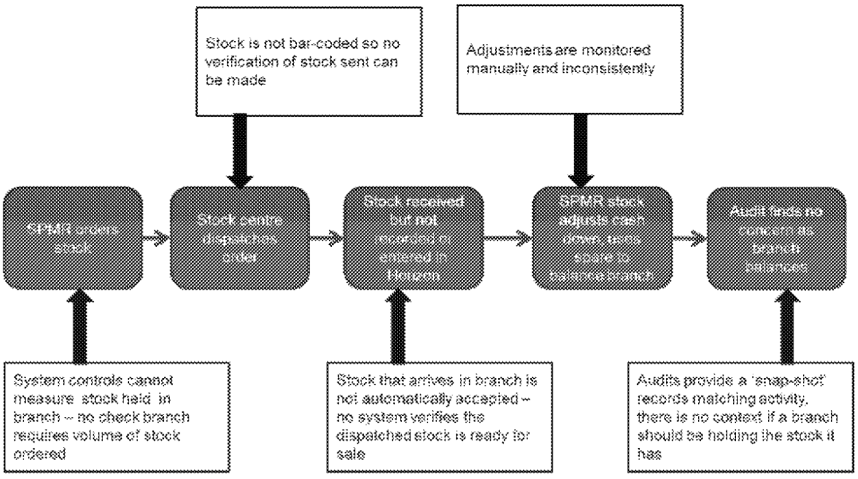


Figure 3-1 Example of how weaknesses in the stock management process can be exploited to hide losses

POL00004408

3.3.2.2 No verifiable, centrally controlled user access to the Horizon system.

SPMRs are permitted to set up system logons for staff without referral to a central control function. Furthermore, there is no limit on the number of logons SPMRs can create except if uncovered at audit. Protocols mean that Horizon log-ons are not unique identifiers and some could be common across many branches. It is therefore difficult to track staff working in one branch and probably impossible to identify users working across multiple branches.

3.3.2.3 ATM reversals

Transfers of cash from the till to ATMs involve transferring physical cash from the Horizon till to the Wincor/Bank of Ireland ATM. The cash transfer transaction should be into a dedicated ATM stock unit and the cash declared on a separate line of the cash declaration each day. Any failure to do so accurately or honestly, as highlighted in section 5.1.1.3, such as reversing ATM payment transactions has been identified as a potential exploit for deliberate fraud as repeated switching, where cash is recorded effectively allows deficits to be hidden. However, in addition to this concern, it has also been observed that the ease in reversing transactions has led to a number of branches inputting an estimated figure on Saturday's 16:30 and correcting for accuracy on Monday. This deviation from the accepted process increases the difficulty in identifying deliberate malfeasance.

3.3.3 Inconsistent audits

The consistency and rigor of the process was raised several times during the Pilot with concerns centred on:

- The adequacy of audits; large losses at branches have sometimes been discovered despite the branch receiving a clean bill of health during a recent audit. This has led to a lack of trust in the auditing process.
- Due to the lack of data and information available to the teams raising Special (urgent) audits, these are currently often poorly targeted resulting in high false positive rates and therefore poor utilisation of resource,
- The apparent leniency towards discrepancies; a discrepancy between expected and audited cash and stock of less than £1000 does not result in an escalation for SPMRs. This does not appear to be an official policy but does appear to be accepted business practice.
- The level of follow up after an audit; it is not clear that on finding a loss and requiring payment from the SPMR's own funds, the Post Office checks that the loss has been made good and not simply reversed by the SPMR in the following month.
- The seemingly opaque nature of suspension decision making. Suspending SPMRs is a commercial as well as an ethical decision at the discretion of the contract manager. Whilst expecting and empowering staff to exercise their judgement is an important principle, the absence of clear and fair disciplinary guidelines leaves the Post Office open to criticism of prejudice and sending mixed messages on toleration of poor business practice.

3.4 Operating environment

3.4.1 Teams interviewed

Interviews with representatives from the fraud team and from the teams with which they work were used to establish a picture of how the Post Office manages and responds to

POL00004408

issues detected in the branch network. Table 3-1 lists the teams with whom interviewees were selected and the topics explored with each.

Team name	Responsibilities	Location	Topics
Customer care centre	Handle in-coming calls from Post Office customers	Barnsley	Team activities and scope, causes of customer complaints, ~~'make good' thresholds~~, monitoring processes
NSBC	Handle in-coming queries from Sub-Postmasters and their staff	Barnsley	Team scope, calls volume, training quality, escalation points
Cash management	Ensure the Post Office branches have sufficient cash to operate	Bristol	Team scope, fraud detection methods, data held, success rates, behavioural traits
Stock centre	Distribute stock to the branch network	Swindon	Stock processes, monitoring procedures, data sets
Non conformance	Call campaigns to reduce non-conformance within the branch network	Leeds	Detection processes, team resource focus, statistical models, conformance rules
FSC (Mails)	Manage payments to the Royal Mail for accuracy	Chesterfield	Royal Mail costs and processes, fraud types detected
Fraud Analysis (Security)	Detect fraud	Chesterfield	Team role, focus, fraud MOs, business processes,
Field support advisor scheduling	Organise audits to occur	Manchester	Audit volumes and processes, outputs, data sets, structure and logic of audit programme
Field support advisors	Undertake audits	UK wide	Role profile, case studies, fraud MOs, experience based information and detection 'tells'
Investigations	Investigate branches suspected of fraud or theft	London	Processes, constraints, case studies, successes, priorities
Cash centre	Distribute cash to the network	22 regional hubs	Cash handling process

Table 3-1: Teams interviewed by this study

3.4.2 Roles and responsibilities

The organisational roles and responsibilities of the teams were documented with particular focus on:

- fraud and conformance detection;
- what information and systems teams use; and
- the key teams they interacted with.

The output of these interviews is shown in Figure 3-2, in the form of an organigraph, showing how teams interact rather than their formal organisation structure. This picture may not be complete as formal understanding and processes do not exist between teams, therefore other individuals may contribute to fraud detection on an ad hoc basis.

POL00004408

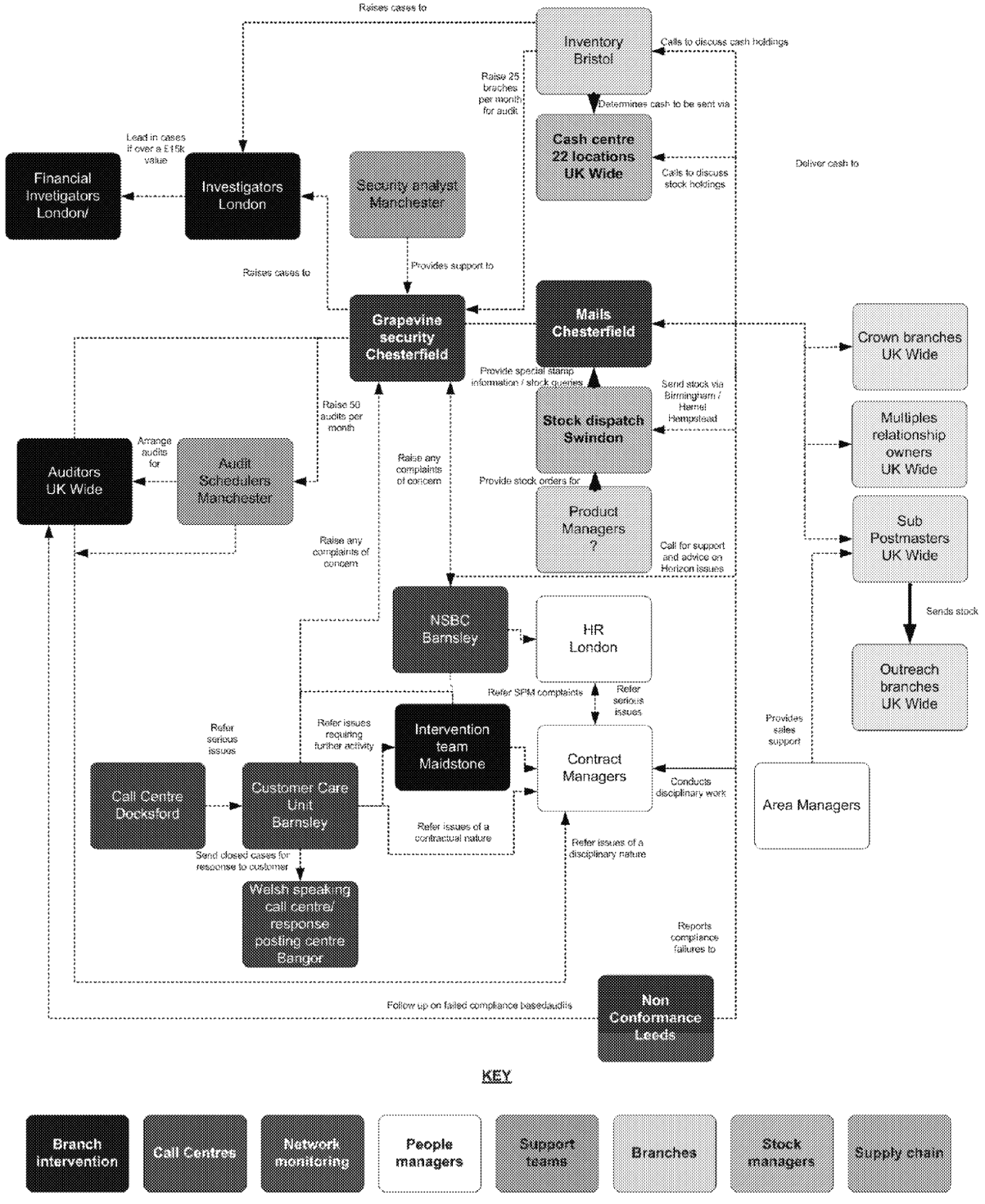


Figure 3-2 Branch supervision organigraph; it shows how teams interact rather than their formal organisation structure

POL00004408

The Post Office suffers from three short-comings in the absence of a formal business process and single data repository to manage branches;

- Detecting poor behaviour is highly inefficient; the picture of branch behaviour is a mosaic constructed by teams only once a concern has been raised during investigations.
- Strategic decision making is difficult; it is not possible to trace or track which branches are of concern to the organisation as a whole.
- The process is brittle; information is dependent on key individuals with specialist knowledge; if these are absent the organisation is less able to respond.

3.5 Post Office Fraud Analysis Security team

Following a restructure in October 2012, the Fraud Analysis team was transferred to Security from Finance Service Centre. Since that time, the team has been re-engineered and it has switched attention from fraud and non-conformance to exclusively fraud detection and changed the division of labour to focus on branches in a region, rather than on specific product and services. However, a number of weaknesses in the team setup were identified which limits its effectiveness. These have been listed below under one of four categories

- Business process;
- Knowledge;
- Technology;
- Data.

3.5.1 Business process

The weaknesses within the process of fraud detection within the Fraud Analysis team limit its capacity to develop a strong detection and prevention programme.

3.5.1.1 Lack of robust controls and records

Probably the most significant area of weakness is the lack of documentation on the expected role of the analyst, the business process to be followed when reviewing and recording a case or the MOs observed.

3.5.1.2 No centralised branch record

The only thoroughly maintained records on branch investigations are the spread sheet of audit outcomes, which, as discussed in 3.3.3, suffers from inconsistency of approach. It is not possible to discern how many branches have been investigated by the team, why they were not referred or whether they should remain on a watch list.

3.5.1.3 Inadequate process and documentation

The team does not have a documented approach and checklist whilst reviewing a branch. Ideally, this should be based both on best practice, what the best performing branches do, and the circumstances of the SPMR. Although the circumstances of each SPMR will be unique they will share features in common with other SPMRs at the same point in the SPMR lifecycle (including; recruitment, induction, training, audit, nine-month review contract exit, etc.) Understanding where in this lifecycle the SPMR is and what is expected of them would enable the Post Office to take assess whether further action was required and what action would be most appropriate. For example, the installation of ATMs is known to change both the cash requirements and the assurance activities of the

POL00004408

SPMR. Currently, no advice exists in how to respond to cash anomalies observed in branches with new ATMs.

3.5.1.4 No concept of risk rating or prioritisation ('Analysts instinct')

Whilst triggers are used to initiate an investigation, such as tipoffs or a targeted programme to reduce known instance of non-conformance, a large number of leads are still generated from manual inspection. High level reports generated on particular transaction types or behaviour are frequently used, some of which contain up to 500,000 results. The effect is to reduce significantly the effectiveness of the analysis performed and its efficiency.

3.5.1.5 Lack of quality control

The combination of lack of process, documentation, and knowledge share means that the quality control both in terms of value and volume of output by the team are weak.

3.5.1.6 Lack of targets or tracking framework

Metrics on the output of the team are neither robust nor conducive to incentivising optimal performance. The principal benchmark used is for the team to raise 50 audits per month, in conjunction with Cash Inventory; the number of branches reviewed to generate these audits is not recorded. Team success is measured by the number of failed audits out of the number raised. Leaving aside the issue of failed audits often being at the discretion of contract managers, this measure does not incentivise the team to act preventatively; rewarding interventions solely based on the failure of a SPMRs career, home and livelihood is likely to be a contributory factor behind the blame culture identified by Second Sight.

3.5.2 Knowledge

The knowledge of the organisation and fraud MOs within the Post Office team is of a high standard. However, due to weaknesses within the team's processes (discussed above) much knowledge of fraud MOs and branch intelligence resides with just one individual. Should an individual be unexpectedly unavailable, as was the case during the study, important information was lost, in the case in point, the ability to review transaction corrections.

3.5.3 Technology

The Fraud Analysis team currently has no dedicated fraud detection technology. The team has developed the 'Fraud checker' to perform automated checks. This is a spread sheet with data drawn from Credence that applies a set of rules to an individual branch's transaction data. This team rely on this tool to initiate the majority of their investigations which has been proven to identify anomalous branch behaviour. However, the tool is also time-consuming to use, provides no historical record, cannot provide trend analysis across branches and cannot track and record outcomes to feedback into a rule-based solution.

Case management is performed using Microsoft desktop applications, including email, word documents or spread sheets. This is far from ideal, especially the absence of a robust audit trail of checks or decisions, document management or case workflow.

3.5.4 Data

The data available to the Fraud Analysis Analysts is limited, degrading the performance of the team. The majority of analysis performed using monthly extracts of Credence data.

POL00004408

However, the team do not have full access rights to all the data required and rely on supplementary data in the form of spread sheets provided by other teams. Where a branch raises concerns, the team will revert to directly accessing source systems, such as POLSAP to review in-balances in the office cash snapshot, or reviewing the IPSL database to ascertain the whereabouts of a cheque, all of which are time-consuming.

Improving team productivity in this regard is a matter of providing better access to the Post Office' data:

- A larger time window than currently provided by Credence, through a more robust and accessible tool;
- Access to declared cash values; in the case of money missing in branch, it is often the false declaration which constitutes false accounting.

Additionally the team lack access to data sources that can be used to risk score;

- Remedy. The Remedy system is used by the Post Office to record calls in the cash management team, where branches can call in and request additional cash, as well as the complaints from the public. In an advanced analytical solution, these would be of interest as warning signs for there being challenges in the branch. To note there is a case in for replacement to a CRM and also a separate compatible one for all FSC.
- EFC. At present two members of the Fraud Analysis team have access to EFC which is a record of the contact between the each SPMR and the Post Office call centre, and the history of previous concerns. This holds enormous value as an indicator of potential issues within branches. During the course of the Pilot, a loss in the region of £45,000 discovered in a branch was subsequently revealed to be managed by a SPMR who had already resigned twice.

POL00004408

4 Post Office data sources

The Pilot was arranged on the assumption that the core data sources below would be made available at the start of the project;

- Branch Database: all transaction data from the Horizon system
- Credence: The Post Office wide Management Information system
- Galaxy: The stock monitoring system
- HRSAP: The HR system

4.1 Difficulties extracting data

Unfortunately these core data sources were not available until the beginning of the third sprint. The Pilot encountered a number of challenges in receiving the data, indicating that the Post Office will struggle to extract more value from its data until the issues encountered by the Pilot are tackled.

- Data managed by several third parties; four procurement and change requests had to be raised. The time taken to respond to these change requests and subsequently to provide the data suggested that making data available to the business was not a key concern when the contracts were agreed.
- Lack of up-to-date data dictionaries. Data dictionaries created when the systems went live had not been kept up to date either on the Post Office or Supplier side. As a result full extracts of each data set had to be obtained, and significant work undertaken to understand the data provided.
- No SLAs for data extracts. The delivery of data was delayed by the lack of SLA provision in the Post Office contracts; the project was therefore required to use a change request process which added further delay to receiving the data
- Prohibitive cost and timescales. In the case of HRSAP and Galaxy it was determined that for a six month project the cost (HRSAP) or the timescales (Galaxy) of delivery were not cost effective, and therefore manual workarounds reliant on individuals within the Post Office had to be found.
- No comprehensive documentation could be identified for customer/supplier/client data captured within the Reference Data Tables ('X Data') in Branch Database. As a result the project was unable to ascertain the rights of Post Office to process and analyse this data under the Data Protection Act, and therefore this data could not be used.

4.2 Alternative sources of data

In order to minimise delay, the Pilot team sought alternative data sources from teams in the organisation to profile with. A complete list of all data sources encountered during the Pilot is provided in Appendix A. Below we discuss the principal proxies used for the core data sources.

4.2.1 The Branch Database and Credence

One of the key limitations of analysis within the Post Office is the main MI system, holds transaction level data for only 90 days before it is summarised. The network team has set up an automatic download of the Credence data available, which now has approximately seven years of data for use in profiling branch behaviour. The Pilot team were able to use this store to take a copy of transaction data of all branches from January 2012 onwards.

POL00004408

Whilst this was extremely valuable as it gave a much longer view than the hosting provider was able to provide, it also was limited in scope.

Some data fields are over-written each day (e.g. cash declarations), and therefore there is no historical data available.

Credence has a number of 'universes'. A universe is a control on what data is available to view by a specific user. Therefore a limited number of data fields were not available in the extract, for example cash declarations by SPMRs.

4.2.2 Galaxy

Data was extracted through the Galaxy user interface. However, this was challenging as the computers which had access to the system were sufficiently antiquated that they could not accept a USB port device. Furthermore, the lack of a data dictionary prohibited investigations into the data.

The Galaxy system is due to be retired; this represents a major opportunity for the Post Office to improve its monitoring as the Pilot team was unable to find a mapping between product records in Horizon and Galaxy so was unable to match what was dispatched to a branch and what it sold.

4.2.3 HRSAP

It was not feasible to extract the HR database via the supplier and therefore was manually extracted through the User Interface after repeated attempts. This was a time-consuming process.

4.3 Other important data sources

The review in [REF 01] identified that much rich intelligence on employees and branches was stored in disparate sources in the Post Office infrastructure. The Pilot was able to identify data sources which could have a significant impact in improving risk profiling.

4.3.1 Electronic Filing System (EFC) held on Lotus Notes

This records interactions between a branch and some teams within the Post Office. This is of particular interest from the perspective of disciplinary notices, rolling debt, resignations and other possible indicators of issues with a branch. Such intelligence would be invaluable in enabling the Post Office to take preventative action. However during the Pilot, the owner of the application could not be identified and how to extract the data was not determined. It has been indicated that the Post Office is moving to a Microsoft SharePoint system, which would allow for easier access. However no migration of historical context will be undertaken, losing the history of a branch.

4.3.2 ATM data

ATM withdrawal data is collected by Wincor, manually manipulated and provided to the Post Office where it is merged in POLSAP to cross-check submitted 16:30. This information should be supplied as an automated feed and made available beyond just the Financial Services Centre, whose responsibility is to account for ATM payments and settle with Bank of Ireland rather than detect error. Such a feed combined with the Horizon data could account for all cash leaving a branch to provide a complete view of each branch's cash management. Additionally a direct data feed would negate the need to cross-check data, and for branch staff to manually obtain and input this data on a daily basis.

POL00004408

4.3.3 Declared cash figures

Currently declared figures, entered by branch staff, are used as the basis for cash dispatch. This information has to be extracted daily from Horizon as it only stores the last entry. Currently the process is relies on manual intervention, given the value to the Post Office in identifying discrepancies within branches it should be automatically stored as an historical record and made more widely available.

4.4 Data quality assessment

The principal data sources identified in 4.2 above were evaluated for data quality in order to identify likely impacts on profiling the data. Table 4-1 below summaries the high level findings of the pilot; a more detailed version is provided in Appendix A.2.The data was assessed along eight quality dimensions:

- Definition: Is the meaning of the data defined and understood?
- Validity: Does the data conform to valid data ranges?
- Accuracy: Does the data accurately reflect the real world?
- Integrity: Does the data structurally link together?
- Consistency: Is the same data consistent across all applications?
- Completeness: Is all the data present?
- Timeliness: Can the data be made available when required?
- Accessibility: Is the data accessible to all who require it?
-

	Credence	HR SAP	Galaxy	Lotus notes	Complaints	Flexible planning	ATM data
Definition	Unclear	Y	Y	Y	Y	Y	Y
Accuracy	Good	Out of date	N/A	N/A	N/A	Y	Manual manipulation
Validity	Y	Y	N/A	N/A	Y	Y	Y
Integrity	Y	Y	Y	Y	Y	Y	Y
Consistency	MDM cause for concern	MDM cause for concern	N	N/A	Some manipulation to link	N/A	Good
Completeness	62 days, declared cash -1 day	150 branches missing SPMR	N/A	N/A	N/A	N/A	N/A
Timeliness	Good (in 62 day window)	Only to selected users	Y	N	Y	Y	N
Accessibility	Limited	Limited	Very	No	No	Y	Very

POL00004408

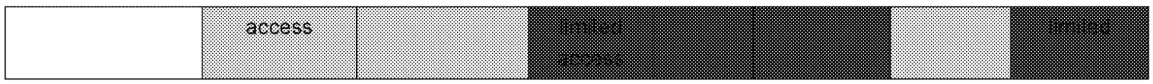


Table 4-1 Data quality summary of principal sources of data identified during the Pilot

POL00004408

5 Data analysis – insight into branch behaviour

It is universally accepted within the organisation that the Post Office is complex. Whilst this does not prevent analysis, it has historically hindered efforts to identify risky branches. The data analysis work stream investigated how data held by the Post Office could be used to identify and prioritise potential fraud, theft or non-conformance within branches. This chapter is divided into two; the first part discusses the observations made about branch behaviour and the second describes the approach used to build a branch risk model

5.1 Observations on branch activity

5.1.1 Complexity and wide-spread non-conformance

The team was directed to two areas of particular concern for the Post Office; the management and tracking of cash throughout the network, and the level of discrepancy between the stock provided to branches and that sold through the tills. The pilot concentrated on analysing cash through the branch network and sales made in branch; analysing stock movements is discussed in 5.1.2.

Below is one example which illustrates how complexity and non-conformance in the network related to cash management not only degrades the performance of the Post Office, but also represents a real and on-going risk of financial loss.

5.1.1.1 Discrepancy between Cash on hand and declarations

One hundred days of transaction data for all branches was analysed to compare the Cash on Hand, "COH", amount and the daily cash declaration which are made by the branch manager or SPMR. In theory the two numbers should always balance, whilst in practice some deviation would be expected to account for errors or refunds.

Of 11,235 branches which had made COH declaration, 6,000 had 10 or fewer days when these two numbers were the same, with 2,000 branches having no days when the two matched, **Figure 5-1**(a). Analysing the average discrepancy for each branch over the 100 days revealed that the average discrepancy between the two figures for 70% of the branches was between +/- £1000, **Figure 5-1**(b). However, the remaining branches showed much larger deviations with more than 1000 branches showing deviations greater than £10,000 or less than -£10,000.

These discrepancies cannot be attributed to purely fraud and non-compliance. Instead they illustrate the considerable challenge faced by Post Office staff in discerning signal from noise. Subsequent investigations into potential reasons for discrepancies identified the following issues:

- difficulties in balancing the till;
- discrepancies caused by ATMs,
- difference in terminology and definition amongst Post Office staff of how to measure COH (whether to include cash in pouches or not);
- branches producing significant numbers of reversals or transaction corrections;
- SPMRs and Crown Branches either fabricating the figure or reducing the figure.

POL00004408

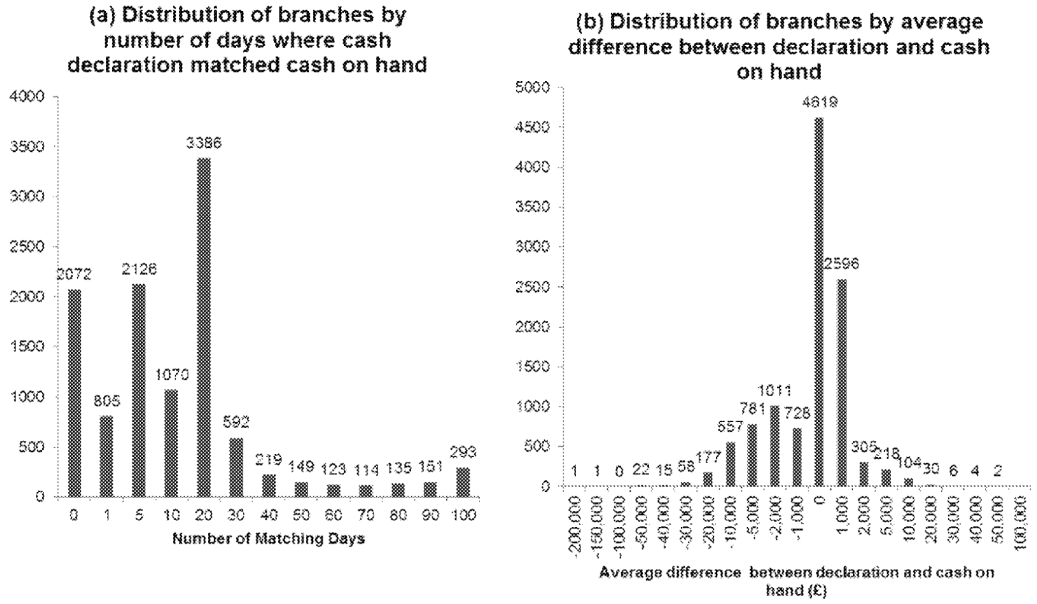


Figure 5-1 (a) Histogram showing the number of days over a 100 day period and 11,235 branches when the manual declaration by the SPMR matched the calculated COH figure; b) Histogram showing the average discrepancy between the declared and COH figure

For the Fraud Analysis team, the last reason is clearly of most concern. Distinguishing between the merely lazy, those leaving cash in open transfer to meet cash holdings targets (a known issue particularly with Crown branches), errors and deliberate malfeasance is too difficult just using this key measure. Furthermore, the Fraud Analysis team had previously identified that some of the branches of most concern were actually the ones with near perfect agreement between the two figures.

5.1.1.2 Cash tracking hindered by process and technology gaps

Discrepancies of such frequency and magnitude as revealed above suggest that multiple gaps in the transactional systems exist where cash goes "missing". Many of the most significant gaps in the system occur when cash is removed from the Horizon till, either to be transferred back to the cash centre, or when a transaction is reversed or corrected (as a transaction correction). Whilst many of these actions are legitimate, the presence of system gaps has led to multiple instances of these types of transactions has historically been linked to losses being uncovered during audits. Below are two types identified during the Pilot.

5.1.1.3 ATM reversals

ATM reversals are a particular form of payment reversal where cash taken out of the Horizon system to fill the ATM is reversed back in by the SPMR. As noted previously it is easy to reconcile Horizon transactions and reversals with ATM transactions as the two systems are not linked. Reversals are a concern as they can enable the branch to regularly switch money between two systems. In one high-profile case this MO was used to hide large losses.

The transaction of 2,523 branches with an ATM were analysed, finding that 883 had made at least one or more reversal, with 121 having 3 or more reversals over a 12-month period in 2012. The presence of an ATM reversal is not in itself risky, although multiple

POL00004408

instances at least indicate a low level of care and attention so the analysis was extended to investigate whether reversals could be matched by value to a REM out to the ATM. This would indicate that money was being cycled between the two systems.

The Pilot identified 33 branches where money appeared to have been systematically transferred between the two. The most systematic was identified as a branch where the SPMR was suspended following large losses being hidden using the ATM.

5.1.1.4 Overstocking

The Post Office faces a number of problems with scratch cards;

- They are a temptation for staff to tamper with them in the hope of winning;
- They can be sold through the retail business rather than the Post Office, with the cash proceeds going to the retail business rather than the Post Office;
- Scratch cards have a sell by date imposed by the lottery operator; any scratch card entered by the branch into Horizon is effectively owned by the Post Office and cannot be returned to the operator. Once the sell by date has been exceeded the lottery cards cannot be sold with the Post Office effectively sitting on a loss.

Sales data for 6,521 branches which show scratch card transactions were analysed over a 15 month period from January 2012. The data was analysed to identify the excess stock that had been entered in Horizon compared with what has been sold. Nearly a third, 2101, had activated at least £1000 more than they have sold over a 15 month period from January 2012. This compares with only an average of £300 excess cards for the majority 4,419 branches. The potential cost to the Post Office of excess stocking was estimated to be £3m.

5.1.2 Untraceable stock

A key issue raised to the pilot team was the lack of tracking between the Post Office's stock dispatch system, Galaxy, and the Horizon sales system. Unfortunately attempts by the Pilot to investigate potential discrepancies between stock provided to branches and that sold were unsuccessful. It was not possible to match stock items between Galaxy and Horizon as the product codes in Horizon had become truncated. The Pilot was not able to ascertain whether a fix for this defect had been found by the Post Office. The Pilot findings suggest it is not possible to check that the stock sent to a branch has been sold.

5.2 Identifying high risk branches

The analysis presented in Section 5.1.1 confirmed that although there are outliers of behaviour, the operational complexity of the Post Office can obscure these. In order to identify risky branches the Pilot attempted to build and refine a model to identify branches likely to be most at risk of encountering losses using previous suspensions as a guide.

5.2.1 Constructing a branch risk model

Generating a risk model requires four concepts discussed below; KRIs, a scorecard, a source data set and a target data set.

5.2.1.1 Key Risk indicators – codifying risk

KRIs are defined as an attribute of an entity which indicates the presence or absence of risk. Making accurate predictions of possible fraudulent activity relies on identifying what KRIs are most closely correlated with fraud. The Pilot trialled a selection of approximately twenty KRIs, to expose non-conformant or fraudulent behaviour.

POL00004408

5.2.1.2 Scorecards

Scorecards apply a weighting to each KRI based on a measure of its importance in identifying fraud. They can also often include additional conditionality based on whether the KRI is triggered in tandem with others. In general, there are two approaches to developing a scorecard; supervised analytics which uses an algorithm to build the scorecard using a known set of outcomes and input data; and the manual approach, where the weightings are decided and adjusted by experiment. Manual scorecards are used when the risk is very well understood and it is relatively simple to identify high risk inputs.

In this case, the number of variables, data volumes and noise is too large so identifying which rules or rule combinations are high risk is complex such that a supervised approach was adopted. Generating the scorecard requires the use of an algorithm-based technique which uses two sets of data; a source set which are used as inputs to the model and the target data set which are used as the outcome, the algorithm effectively works out an equation to link input data to the outcomes.

5.2.1.3 Source data sets

The source data sets included the transaction data (see 4.2.1), transaction corrections (also 4.2.1) and cash declarations (4.3.3). Both discussions with the business and preliminary investigations had shown that transaction corrections were strongly correlated with suspensions.

These data sets were manipulated as follows for inclusion in the model:

Transactions – aggregated and turned into branch-level measures, and used to calculate values attributed to the candidate KRIs for the model and the result standardised to per-million transactions values.

Cash declarations –used to measure the discrepancy between the reported and the values generated by the Post Office.

Transaction corrections - each type is aggregated to produce a set of statistics including the average amount, maximum amount, minimum amount, total amount, total number of positive transactions and total number of negative transactions.

Non Crown branches – the years in service of the SPMR is calculated.

5.2.1.4 Target data set

The Audit outcome spread sheet discussed in 3.3.3 was used as the target data set. Although not without its faults it does represent the best data set available to identify branches found to be of greatest risk to the business. This data set is also used to identify the date when the audit takes place; only source data from before this point is used in the modelling process

5.2.2 Model performance measurement

Once a model had been generated which passed a preliminary statistical test (simply how well the model using the input data could predict the outcome data) it was used to score all branches using data from after they were audited. The performance of the model was tested in two ways:

- historic back testing, where the new model is tested on audits not used to build the model, whose results are shown below;
- user validation, where highly-scored branches are presented to members of the Fraud Analysis team who investigate the branches in turn and subsequently decide whether or not to raise an audit against the branch.

POL00004408

At the time of writing user validation was on-going, however, the results of historic back testing are available.

5.2.2.1 Historic back testing

The results presented here used a model generated from audit data from April 2012 – March 2013. All branches were scored based on their transaction history for the period April 2013 – June 2013 for which it was possible to obtain actual audit results. This enables comparison between the model and actual events. The model was also used to score the branches for the user validation exercise mentioned above.

The comparison between the model and actual events is shown in **Error! Reference source not found.**, below, as two superimposed graphs:

- a histogram showing the distribution of branches by probability of failing an audit, in discrete ranges from 0-100% (left hand axis);
- a line graph shows the cumulative percentage of audit failures from the three month period against the risk score of each failed branch (right hand axis).

The histogram is divided into two parts; branches below 5% probability of failing an audit is classified as "low risk" (light coloured bars), whilst those above have been classified as "high risk" (dark bars). A value of 5% value was used as this is currently the average audit failure rate across all audits performed by the Post Office; branches with a risk greater than this are therefore of more concern to the security team.

Together the two graphs indicate:

- the efficacy of the model in identifying high risk branches, by indicating how many of the suspended branches were classified as high risk; and
- the model efficiency, the number of branches in the high risk sections that require investigation.

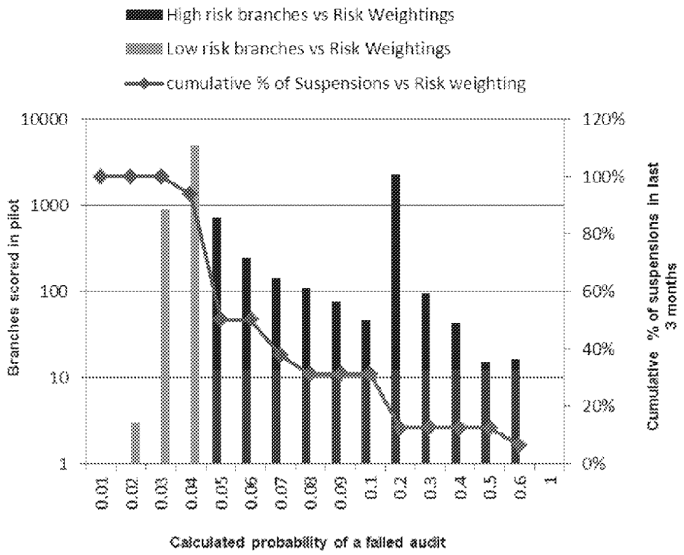


Figure 5-2 Performance of new model in (a) (bars, left axis) distributing the branches across a spectrum of probability scores with low risk branches (with less than 5% chance of failing an audit) and high risk branches (darker bars), note the scale is logarithmic; b) (line, right axis) fraud score of failed branches as a cumulative percentage

POL00004408

The model classifies approximately 50% of the failed audits are correctly classified as high risk with approximately 39% of the branches overall categorised as high risk.

To improve the model the Pilot investigated the false negatives (low scoring branches which failed an audit) and false positives (high scoring branches which passed audits).

- False negatives – reasons for incorrect low scores
    - Some branches fail due to on concerns raised by other parts of the Post Office, e.g. poor financial health of the retail business, suspicion of mails fraud and removal of cash from the safe;
    - Some failed due to issues not currently captured by the KRIs, e.g. non return of unusable notes which would require data on denominations which is not currently captured
- False positives –reasons incorrect high scores
    - Incorrect data supplied to the Pilot
    - Many of the top scoring branches were BFPO which have not been audited but which show some of the high risk characteristics of failed branches (as the model does not have any audits for BFPOs it does not adjust for the different business characteristics).

5.3 Investigations into what causes branches to become risky

Whilst the model above has been shown to risk score branches, it is difficult to discern from the model whether there is any underlying pattern of behaviour. For example, whilst the model identifies the weighting to be applied to each Key Risk Indicator and what transaction corrections were most closely correlated with failed audits, it does not explain help to explain whether there is a correlation with type of branch or products sold.

In order to cast light on the factors which drive good or poor behaviour a number of modelling techniques were used to categorise and separate branches into groups of similar behaviour. In contrast to the techniques employed above in these exercises there is no target data set; there is no right answer. These techniques are sometimes used to segment customer behaviour in a retail environment. Two separate techniques were used:

- Kohonen clustering – which was used on all branches
- Hierarchical clustering – which were used on sub sets of the data to provide greater clarity

For the purposes of both studies the definition of a failed audit was adjusted to take account of the difficulties encountered with regard to recording outcomes and the commercial decisions of contract managers, and the fact that only Sub Post Offices are likely to record a failed audit as a suspension. The definition of a failed audit was therefore deemed to be one or more of:

- Record of SPMR being suspended;
- Record of audit escalation;
- A financial discrepancy at audit of more than £3,000 for all branches except Crown branches;
- A financial discrepancy at audit of more than £5,000 for Crown branches.

POL00004408

5.3.1 Kohonen clustering: how similar branches are to each other

Kohonen clustering uses an algorithm to group items by their characteristics into one of a predetermined number of groups. The groups are arranged as a square matrix of groups, where groups nearest each other are most similar. The algorithm will then further cluster the groups together to show the major boundaries in the data set.

In the case here, after some experimentation the branches were sorted into 81 different groups. The data used to sort the branches included Key Risk Indicators, audit results, and transaction corrections. The results for this are shown in Figure 5-3 and Figure 5-4 which represent the data in two different ways.

Figure 5-3 plots the branches in their original Kohonen map positions to show how the different clusters relate to each other. The data for this map is also provided in Table 5-1 on pages 32 and 33. The map shows that as expected the Sub Post Offices dominate the map with the Crown offices and Multiples and Chain branches interspersed between them. There are a small number of branches at the bottom left of the matrix which are quite different in character from the other branches.

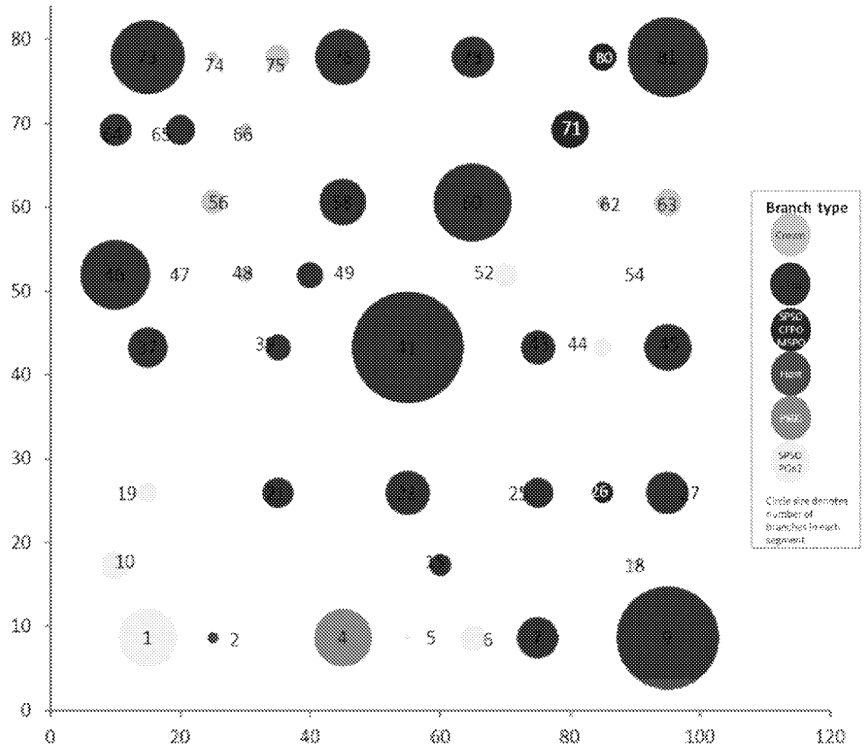


Figure 5-3: Kohonen map for all branches, where size of circle indicates the number of branches in each group and the distance between two groups indicates how similar they are to each other. The colour of the circle denotes the type of the majority of the branches in that group. The number on each circle denotes its grouping for reference which are provided in Table 5-1

POL00004408

The data from the previous graphs is provided in Table 5-1, showing the size of the group, the number of branches in the group, the percentage of branches that failed an audit and the percentages of branches which did not have an audit record. A list of all branches and the group they have been assigned to is provided in Appendix C.

Group reference	Grand Total	Percentage failures	% unaudited	Average annual transaction
1	492	0%	100%	£ 143,144.32
2	15	0%	100%	£ 122,198.81
4	461	0%	100%	£ 7,066.38
5	2	0%	0%	£ 29,446.21
6	99	14%	58%	£ 550,713.11
7	233	5%	64%	£ 371,726.00
9	1446	17%	69%	£ 1,290,398.86
10	118	5%	0%	£ 198,242.66
15	72	24%	49%	£ 2,353,864.81
18	15	8%	20%	£ 1,647,039.00
19	64	2%	0%	£ 398,329.52
21	130	12%	75%	£ 80,985.23
23	278	21%	60%	£ 887,476.71
25	129	12%	0%	£ 1,561,858.83
26	61	12%	3%	£ 1,942,776.11
27	247	19%	60%	£ 1,408,621.75
37	217	21%	60%	£ 918,648.46
39	90	14%	77%	£ 270,857.79
41	1708	8%	68%	£ 1,115,070.47
43	160	12%	0%	£ 818,921.88
44	52	12%	0%	£ 885,128.35
45	309	14%	59%	£ 1,056,670.74
46	671	23%	64%	£ 3,041,499.14
47	1	0%	0%	£ 1,302,210.62
48	29	6%	41%	£ 4,116,284.83
49	96	5%	55%	£ 1,040,878.10
52	95	10%	2%	£ 882,487.55
54	3	33%	0%	£ 308,427.50
56	79	12%	38%	£ 4,726,164.75
58	295	20%	71%	£ 3,376,949.24
60	831	7%	67%	£ 720,754.12
62	27	5%	19%	£ 3,931,162.15

POL00004408

63	106	5%	47%	£	2,494,114.34
64	146	9%	62%	£	1,183,185.90
65	125	34%	42%	£	2,946,084.57
66	27	0%	33%	£	4,572,482.61
71	194	16%	55%	£	1,836,392.42
73	743	22%	64%	£	3,255,674.10
74	17	22%	47%	£	3,235,428.94
75	82	4%	37%	£	2,808,862.71
76	421	24%	64%	£	2,704,644.67
78	246	12%	66%	£	444,340.02
80	105	8%	1%	£	1,362,792.76
81	893	12%	69%	£	1,265,018.29

Table 5-1 Summary of branch clusters, with clusters with a failure rate greater than 20% highlighted

Figure 5-4 shows a second way to represent the data in Table 5-1 by plotting each branch group along an axis of average annual transaction value processed by branches in the group and the percentage audit failure rate. This is a way of showing the risk profile of the branch groupings. In this configuration it becomes more apparent that the different types of branch types represent very different levels of risk to the Post Office.

The graph is split into four quadrants divided by the average transaction value for all branches and the average audit failure rate for all branches. Groups in the top right quadrant therefore represent high risk, high volume branches, where the most money is at risk.

Most of the Crown branches are in the top left quadrant, transacting far more than any other branches and experiencing far less audit failure far less than any other type. However, a small group of Crowns (Group 74) does show a similar risk profile to the high risk SPMR groups in the top right quadrant.

The SPMR groups are effectively split into two; a low risk, low transacting set of branches and a higher risk and higher transacting set of branches. Of most concern to the Post Office is Group 65, a mix of Sub Post Offices, Multiple and Chain branches which appear to be extremely high risk.

Of most concern to the Post Office is that the graph appears to show that Sub Post Offices substantially increase in likelihood of audit failure as the number of transactions increase. This relationship is not seen for Crown branches. It appears that the Crown branches are much stronger performers in terms of conformance than the Sub Post Offices. This analysis indicates that selling Crown branches to franchises, whilst appearing to represent good value for money for the Post Office, could lead to the Post Office increasing its risk of financial loss and non-conformance.

POL00004408

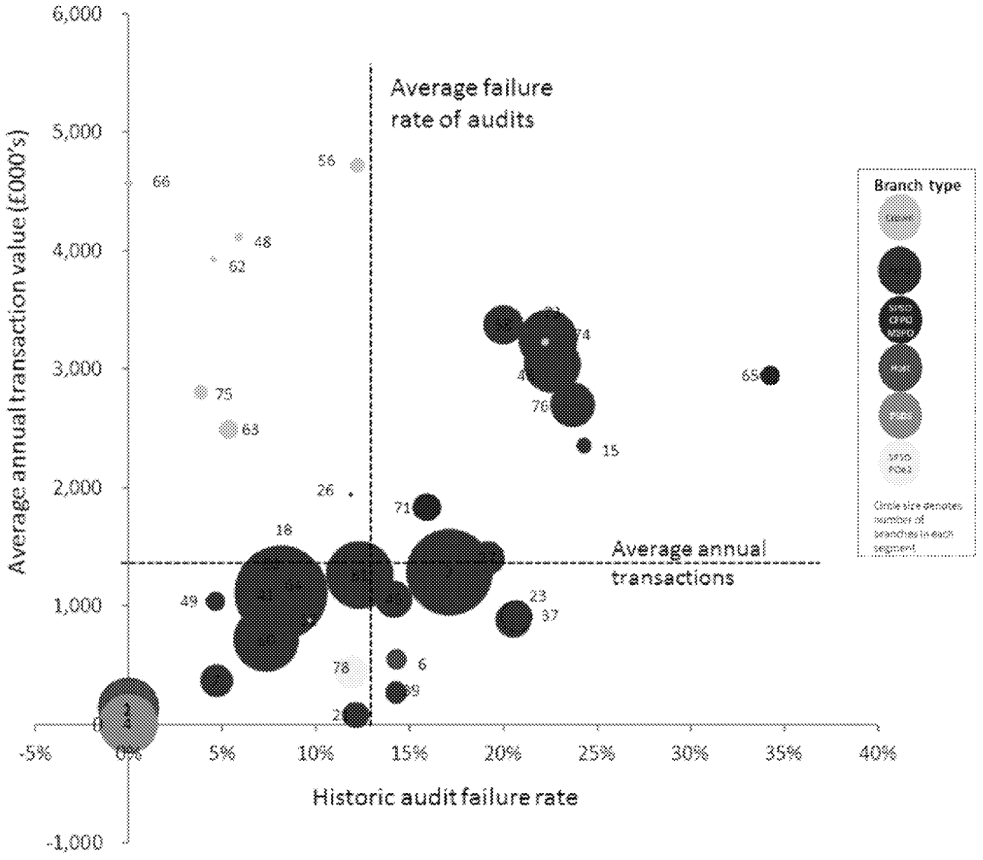


Figure 5-4: The same Kohonen groupings as before but plotted by the average value of transactions over one year for the group and the historic failure rate of audits. The size of the circle again indicates the relative numbers of branches in each group. Grouping in this way indicates the relative risk and the relative amounts of capital at risk for each group.

5.3.2 Hierarchal clustering: how different branch types fail audits

Hierarchal clustering is a more computational intensive technique and therefore more suited to smaller groups of entities. Separate computational tests were run for different types of branches, using transaction corrections, presence of ATMs, Key Risk Indicators and audit results to investigate what the key discriminating factors in grouping branches together. For each result the team observed which measures were most important in determining the behavioural characteristics of each segment

5.3.2.1 Crown branch behaviour

Crown branches were found to be split into four segments as shown in Table 5-2 below. In contrast to the other segments, the absence of an ATM did not lead to an improvement in the branch conformance. High non-conformance appears to be correlated with Scratch card Transaction Corrections and Foreign exchange TCs. Please note the cluster name is for reference to the underlying analysis only. The table is ordered in decreasing audit failure rate

POL00004408

Cluster name	Description of key characteristics	No. of branches	% of failed audits
Crown_3	No ATM, Foreign Exchange TC Scratch card TCs	36	11%
Crown_1	Average profile for Crowns	82	6%
Crown_4	High spoilage, Low Online Banking Low "Other" TC	64	5%
Crown_2	High ATM Retracts, Low on other ATM TCs, High Cash Rems To Branch, High Stock Discrepancies	44	0%

Table 5-2 Crown branch segments

5.3.2.2 Sub Post Office branch behaviour

SPMR failure rates appear to be very much determined by which services they do not offer. Removing the ATM reduces the risk of SPMR being suspended, as does the presence of Lottery tickets, Santander services and DVLA processing.

Cluster name	Description of key characteristics	No. of branches	% of failed audits
SPSO_7	No DVLA	322	23%
SPSO_8	All products and services	308	19%
SPSO_1	No Camelot sales	238	17%
SPSO_2	No ATM, No DVLA	566	14%
SPSO_5	No ATM, No Santander, 50/50 Camelot 50/50 DVLA	216	11%
SPSO_3	No ATM No DVLA	849	10%
SPSO_6	No ATM, No Camelot, No DVLA	441	9%
SPSO_4	No ATM, No Camelot, No DVLA, No Automated payments, No Government, No Pay Station, No Santander, No NSI, No Fx Longest Serving SPMRS	121	1%

Table 5-3 Sub Post Office branch segments

POL00004408

5.3.2.3 Multiple Sub Post Office behaviour

Multiple Sub Post Offices are by far the weakest performers in terms of conformance. Once again, the absence of the ATM appears to reduce the risk, however, the failure rate is still considerably above the average, which is about 14%.

Cluster name	Description of key characteristics	No. of branches	% of failed audits
MSPO_3	High stock discrepancy,	24	50%
	Unpaid cheque TC		
MSPO_1	Does everything	58	36%
MSPO_2	No ATM	112	21%

Table 5-4 Multiple Sub Post Office branch segments

5.3.2.4 Chain Franchise behaviour

CFPO performance is markedly lower than SPSOs, with only the absence of an ATM appearing to reduce branch risk.

Cluster name	Description of key characteristics	No. of branches	% of failed audits
CFPO_1	Lower TCs than CFPO_3 but high out of hours	79	33%
CFPO_3	High Santander TCs	28	32%
	FX corrections		
CFPO_2	No ATM	76	9%

Table 5-5 Chain Franchise Post Office branch segments

5.3.2.5 Key factors in determining risk

Apart from the Crown branches, the most important factor in determining which cluster is high risk appears to be the presence of the ATM, Santander processing and Lottery tickets. Furthermore, the high level of failure amongst CFPO and MSPO is an important risk, especially when compared against the performance of similar sized branches such as Crown Post Offices.

POL00004408

6 Case studies

This chapter presents some select case studies encountered during the Pilot to highlight the need for change across the Post Office in policy and process, system design, monitoring and team performance.

6.1 Non-conformance

Detica has encountered multiple examples of non-conformance across the network; whilst in all cases there is a measure of culpability on behalf of the SPMR or branch manager, many times the underlying reasons driving the behaviour are compelling.

6.1.1 Non-conformance to serve business customers

During the initial stage of validation, three high scoring branches were observed with very similar profiles. All had long serving SPMRs, in large urban areas (Bristol, Birmingham and Glasgow). All three were identified for concern due to regularly adjusting high amounts of cash to cheques. All three were closely investigated, including viewing cheques scanned by IPSL to verify they were legitimate and not paid in from the SPMR s' personal accounts which would have indicated the SPMR was surreptitiously borrowing money from the Post Office and paying back.

In all three cases the cheques were paid by car rental firms. It appears all three had unofficial arrangements with car rental firms. The Post Office would process the transactions as cash throughout the month, and then settle at the end of the month with the car rental firm. Once the cheque was paid, the cash transactions were reversed. This arrangement is very profitable for the Post Office and SPMR. However an audit during the month would have exposed a large loss in branch, potentially resulting in a suspension.

6.1.2 Non-conformance related to un-tracked stock

At the end of February Christmas stamps should be moved from special stamp stock unit to be sold as regular stamp units. After an audit showed one branch with approximately £12,000 in Christmas stamps in stock in August, it was identified that approximately 1000 branches were still holding Christmas stamps six months after their withdrawal date.

6.2 Ineffective training

Losses from ATMs have been one of the major concerns of the Post Office during 2012-2013. The Post Office has experienced high losses from both SPMRs or branch staff hiding losses through repeated reversals between the Horizon till and the ATM, or via malicious retractions. It is therefore critical that the Post Office ensures all Post Office staff are fully aware of all issues and workings of ATMs.

Two branches recently audited as part of the Pilot referrals showed shortfalls where in each case the cause was attributed to not understanding how the ATM operates. Both SPMRs claimed that the only training received in how to use the ATM was provided by the installation engineer.

6.3 Ineffective auditing of branches

The variability and potential unreliability of audits has been a theme repeated during the Pilot. One branch raised for unusual behaviour during the Pilot validation was not audited as it had been audited in the previous few weeks, receiving a clean bill of health. Rather than perform another audit, a follow up call was arranged with the branch manager. No

POL00004408

further action was taken. However, towards the end of the Pilot we were informed that yet more concerns had been raised at the branch, and another audit was being arranged.

POL00004408

7 Report conclusions and recommendations

7.1 Overview

This chapter lists the key conclusions of the Pilot, makes recommendations to tackle the challenges facing the Post Office and provides a roadmap of change for the security team to implement the recommendations.

7.2 Report conclusions

We have identified four broad areas of particular concern:

- Widespread non-conformance to Post Office policy and processes by branches together with an institutionalised acceptance that errors and non-conformance exists;
- Complexity and fragmentation of information systems which hamper efforts both to gain an insight into branch behaviour and take effective and efficient action;
- Ineffective process, policy and working practice across the various Post Office central teams to gather information, prioritise and act in a co-ordinated manner.
- Technology available to central teams are not fit for purpose; analysis of large data sets is performed on an ad-hoc basis of data subsets copied into Excel and tasking of teams is initiated and managed through email.

7.2.1 Widespread non-conformance

Post Office staff are aware that non-conformance and deviation from expected business practice amongst branches exists and is widespread. What is not visible is the extent and frequency, and therefore the appropriate business priority to address the underlying issues cannot be articulated.

The root causes of incidents of non-conformance appear to be the complex and fragmented systems (described below), exacerbated by a culture which has accepted that workarounds are inevitable. Whilst in isolation non-conformant transactions may appear to branch staff to be insignificant, when multiplied across a network with some two billion transactions per year and 11,700 branches, the impact on the security team is to obscure non-compliance and fraud amongst operational noise.

7.2.2 Complex and fragmented systems

Post Office systems are not fit for purpose in a modern retail and financial environment. Our primary concern here relates to difficulty in reconciling information from multiple transaction systems both in terms of timeliness, structure and access. Several examples highlight our case:

- Product codes for items in Galaxy and Horizon are different in each system, with many to one mapping of products from Swindon to Horizon meaning it is not possible to identify all products individually end to end. During the Pilot it was not possible to either match the two systems or ascertain whether any team in the Post Office had been tasked with or had succeeded in doing this.
- Cash declarations which are manually entered by branch staff and Cash on Hand, calculations automatically generated in Horizon should match. These differ frequently and in a significant minority of cases these differences are extreme. Of 11,235 branches analysed over a three-month period, 6,000 had 10 or fewer days when these numbers were the same, and for 2,000 branches, these figures never

POL00004408

matched. Failure on this scale indicates that there is a fundamental issue with the process or controls in place around cash balancing. As if to underline the point, a Key Risk Indicator recognised by both the Fraud Analysis team and the Pilot, is that of a branch that is too good at matching these numbers; rather than branches that balance perfectly every time being seen as 'good', this is seen as an indicator of branches that are 'bad', with several cases of perfectly balancing branches found to be fraudulent.

7.2.3

7.2.4 Ineffective process, policy and business practice in central functions

Efficient and high-performing central teams are the cornerstone of a well-run franchise network, enabling the centre to monitor and control its branches. Although Pilot investigations were pre-dominantly focused on the Fraud Analysis team, several other teams within the Post Office were also observed to fall short of industry standard practice. In particular it was observed that;

- There is no process for centrally managing information or tasks across branches except in relation to organising audits.
- Records of branches investigated or targeted that did not warrant an audit are not kept, or are not kept in an accessible manner; it is simply not possible to discern how many branches had been passed as operating correctly by teams across the business, nor how many had not been subject to no checks, concerns or outbound calls in any given month.
- The Fraud Analysis team does not have a fit for purpose tracking framework; progress is only measured by the number of audits raised by the team resulting in suspension; there is no incentive to operate preventatively.

7.2.5 Technology available to central teams are not fit for purpose

The technology available to the central teams is not fit for purpose and inhibits the execution of their activities in three key areas:

- Investigation into a branch's behaviour using all data sources is time-consuming and can only be performed manually into individual branches.
- No tool exists to share tasks or collate case files either between members of the Fraud Analysis team or with the teams with whom they work. Teams do not know which branch is of concern and cannot share information easily.
- Knowledge management on branches is widely dispersed with useful information held in hard to reach data stores where ownership is not commonly known. By way of example, although an owner was located, and read only access could be obtained, in six months neither Detica NetReveal nor Post Office staff were able to find a way to extract all the data in bulk from the Electronic Filing Cabinet (which some teams use to collate information on the interactions they have with branches) so that it could be integrated into an easily searchable format.

7.3 The case for change

The findings of this report suggest that the existing Security team's approach is not sustainable. Most pertinently, the team already struggles to identify and manage non-conformance in the network and this on the evidence above will only get worse; some of the best performing branches for conformance, Crown branches, are being sold off to become part of what is currently the most non-conformant – multiples or chain franchises.

POL00004408

Furthermore, in order to become profitable, the Post Office has made a strategic decision to sell more products and services. From the evidence of the Pilot it is the addition of more products and services which trigger failed audits. Perhaps many in the Post Office will feel this is self-evident and inevitable; more products inevitably means more applications and equipment for Post Office staff to manage and the more of these there are the easier it is for those staff to make mistakes. However, there is no reason why this should be so; the Post Office may be unique, but it is not uniquely complex. The Post Office needs to adapt it approach to enable more products and services profitably and correctly, with rigorous oversight of branches and stronger support for Post Office staff.

7.4 Recommendations

In light of the Post Office's strategy to achieve transformation in terms of modernisation, growth and customer excellence, the aim to achieve profitability across the Crown network from 2015/16 and the reduction of the Government Network Subsidy payment from the current financial year, it is vital that Post Office implements a robust strategy and solution to reduce non-conformance and fraud opportunity across it's complex network. We have devised these recommendations to enable the Post Office to tackle the challenges it faces today and adapt to the future, particularly the introduction of more financial services and Front Office if Government products which will pose a greater fraud risk.

The report recommendations have been divided up by the section of the report to which the issues they address are raised.

7.4.1 Business Context

See Chapter 3

7.4.1.1 Business practice

1. The following recommendations illustrate that some re-design of the Horizon system is of critical importance for the Post Office in particular:

    i. The engagement of users from the branch network in the design to simplify the design to reduce the number of mis-keys;
    ii. A re-design of system or process where data illustrates that it is too difficult for users to get it right
    iii. The removal as far as possible of multiple paths to process the same transaction or function;
    iv. Remove the ability to keep cash or stock as open transfers;
    v. Active warnings to inform users when cash has been put in pouches but has not been delivered to the cash centre;
    vi. Automatic scanning in of stock and stock volumes as is the case with cash;
    vii. ATM transactions should be integrated fully with Horizon;
    viii. Cash declarations require greater granularity to track note and coin denominations;
    ix. Cash declarations are currently over-written daily, and therefore there is a lack of audit trail for the business. A daily data extract exists from Fujitsu for Cash Inventory and is loaded into Flexible Planning, but is not available elsewhere - individuals across the business extract the data daily, but there are gaps on non-working days (i.e. weekends)
    x. Bureau de change should be managed fully in Horizon, including tracking note and coin denominations.

POL00004408

2. Within branches, a number of devices exist that process transactional and payment activity (e.g. Post & Go, Camelot, utility key top-ups), which are not fully integrated into Horizon, and where cash has to be manually brought to account over the Horizon terminals.

3. Review and re-publish policies on non-conformance to establish a clear set of business practice guidelines:

    i. Define what should be corrected by education/training and what constitutes non-conformance and fraud and what the subsequent penalties for infractions are, particularly for the most prevalent issues i.e.:
        a) Cash kept in open transfers overnight;
        b) Declaring a '1630' ATM figure at a time other than 16:30;
        c) Not accounting for Santander business by 7pm each Wednesday;
        d) Inaccurate cash declarations;
        e) Not returning excess cash
        f) Not dispatching cash by the next available pick up date;
        g) Lack of security around logons
        h) Not dispatching cheques on the day they are accepted.
    ii. Work with the branch network users to identify areas of existing "work around" which are performed to help customers e.g.
        a) Abuse of 'other postage sales' to accept card payments (for instance for retail products or to avoid the requirement to take photo ID for Bureau transactions).
        b) Serving EBay customers as though through other postage then reversing and issuing postage labels later.
        c) Serving car fleet business customers who appear to pay on account by reversing individual cash transactions and later processing one bulk cheque payment.

4. Review, clarify and re-publish policies and processes on audits particularly with regard to losses and the trigger for suspensions:

    a) Recording the complete audit process not just the outcome, particularly in relation to where no suspension was enacted but where additional actions before the audit was passed;
    b) Increase the number of audit outcomes to include those where a contract manager was involved.
    c) Record additional audit outcomes where risk or non-conformance is found, for example excessive cash held, personal cheques on hand, values in suspense.

5. Verify and check all staff who will work in the Post Office branch network

6. Institute a centrally controlled logon system for Horizon users.

7. Ensure that each Horizon user across the network has a unique log on ID

8. Review with the SPMR and Crown communities the training, personal support and technology available to branches in order to identify pain points.

9. Benchmark Post Office security and monitoring procedures against other retail and financial business particularly with respect to:

    a) Stock ordering, tracking and management;

POL00004408

b) Cash management and monitoring of transactions made at tills;
c) Management of ATMs;
d) Use of CCTV to monitor till activity.

10. The Post Office should undertake a review of its stock distribution and management system including a cost benefit analysis of using a commercial partner to distribute stock on its behalf, including the value in tracking stock from receipt at the distribution depot to the point of sale.

7.4.1.2 Operational teams

11. The central team structure and operating model requires an overhaul to make it less reactive, including reducing the number of teams through merging closely-related functions. This will prevent gaps in knowledge between teams and re-work across the Post Office and prevent multiple contacts to the same SPMR by ensuring that decisions re. contact are made with the 'whole picture'.

12. Provide the central teams with one workflow tool and one knowledge-capture tool to coordinate activity across all teams in relation to branches.

13. In the short term, open up access to Remedy to all Fraud Analysis team members and allow the team to take a complete extract of Lotus notes (also known as Electronic Filing Cabinet (EFC) rather than just single files as is the case currently.

7.4.1.3 Fraud Analysis team

14. Document the role of an analyst and define the business process to be followed during an investigation, including case decision and issue escalation processes.

15. Refine the team structure and expand training to take advantage of the knowledge of the whole team and reduce the dependency on single points of failure.

16. Introduce a concept of quality control and rigour in the investigation process, including a review of staff decisions.

17. Introduce a process for managing branches by risk and business profile.

18. Introduce a target and benefit tracking system based on both the number of branches worked and the number of correct referrals.

19. Change the concept of a correct referral to include cases preventative outcomes not just suspensions.

20. Audit, cash management and Fraud Analysis teams should be encouraged to work more closely together, preferably ahead of the roll-out of a combined case management system across all central teams.

21. Implement a robust autopsy process for cases where significant loss or significant operational deficiencies have been identified that includes key stakeholders from across the business, to ensure that preventative controls across the business can be improved

22. Introduce a new reporting structure for the team to track progress.

POL00004408

7.4.1.4 Technology to combat fraud

23. The fraud team require a dedicated fraud detection system to automate the detection of fraud across all branches in order to eliminate much of the time staff currently spend manually scanning through and manipulating data.

24. The fraud detection system should build on the success of the fraud checker spread sheet in particular it should:

    a) Provide a longer time window into transaction data;
    b) Provide access to declared cash values;
    c) Automatically ingest data from multiple sources to reduce the overhead of loading individual branches;
    d) Prioritises branches by level of risk;
    e) Provide an audit trail of previous investigation activity
    f) Enable teams to manage cases.

25. The fraud detection system will need to be expanded to cover analysis of customer behaviour, particularly if the proposed expansion into offering more financial services and Front Office of Government products goes ahead.

7.4.2 Data sources and data quality

See Chapter 4

26. Undertake a review of data requirements across the central business functions and re-design MI with a focus on providing access to the right information in a timely fashion.

27. Ensure new contracts for data sources explicitly include requirements relating to data access and MI for users.

28. Undertake a review of the governance of data sources across the Post Office; each system should have a designated owner who is responsible for data quality including ensuring data entries across systems can be matched (e.g. Galaxy and Horizon).

29. Ensure data from the Remedy and Lotus systems is migrated and not lost when a new system is procured.

7.4.3 Detecting branch behaviour

See Chapter 5

30. Wherever possible the acquisition, aggregation and manipulation of data should be automated.

31. Introduce technology to automatically track stock between stock management and till system.

32. Introduce an automated feed between Horizon and Wincor to enable monitoring of both sides of the ATM cash dispense and transfer process, and negate the need for branch staff to access the ATM daily to extract dispense figures and then manually input into Horizon (and thereby eliminating failure to perform process and mis-keys).

POL00004408

33. Introduce automated same-day reconciliation between ATM and Horizon transactions at the end of each day to ensure cash can be tracked. Branches should be immediately informed if cash moved from the Horizon till for use in the ATM is not available for use by the ATM.

34. Introduce a robust process for capturing and acting on reversals and transaction corrections where behaviour is above normal.

35. Investigate and reduce instances of discrepancies of cash on hand and declarations.

36. Introduce a system to automatically track over stocking of items, particularly scratch cards, including those branches that activate all scratch card packs on receipt, rather than as required.

37. Introduce a system to automatically profile and risk-score branch activity.

38. Introduce a system that can track and profile anomalous individual activity, e.g. log on to Horizon/transaction processing outside branch trading hours, log on activity that indicates shared passwords, anomalous transaction activity by one individual

39. Introduce a system that detects fraudulent behaviour at the earliest opportunity and allows Post Office to implement preventative measures and controls, rather than requiring resource deployment and costs in respect of investigation and recovery

7.5 Roadmap for the security team

The purpose of the roadmap is to provide a potential route forward for the Post Office to modernise its response to fraud and non-conformance to be comparable to related industries such as insurance and retail banks.

The Security team will support the Post Office's goal of being cost neutral during 2016 through:

- Joined up working with audit, cash, stock, investigators and contract managers to support branch network in their day-to-day business;
- Risk-based targeting of branches to identify and intervene more rapidly in branches which are deviating from accepted business practice;
- Providing one place to access to data, aggregated at the right level, to enable staff to make rapid decisions;
- Improved working practices and higher expectations for the Security team.

7.5.1 Timeline for key changes

Figure 7-1 highlights the key changes the Post Office will undergo over the next three years. The challenge for the Security team is to develop its capabilities in parallel with these to ensure the Post Office can respond appropriately. The key milestones and the implications for the security team are described below.

7.5.1.1 Second Sight Review

An interim report by Second Sight, and the accompanying commentary by unions and parliamentarians, suggests that the Post Office will be challenged to respond comprehensively and openly about the changes to be enacted when the final report is published. The Post Office will be required to demonstrate the changes it will make to improve the working relationship with SPMRs, including adequate training, support and guidance, and a consistent approach across the business.

POL00004408

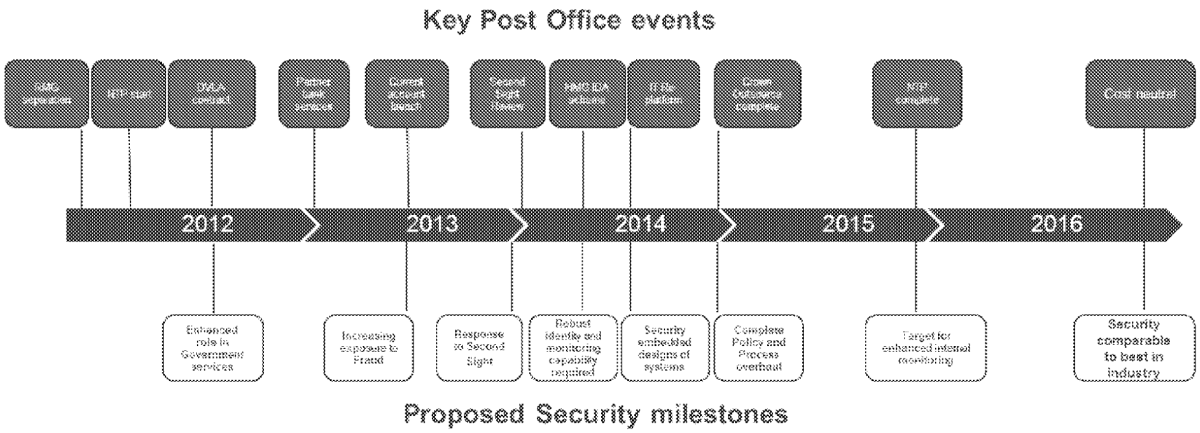


Figure 7-1 Key milestones for the Post Office (top) and corresponding milestones for the security roadmap (bottom)

7.5.1.2 IT platform migration

The Pilot has identified multiple gaps within the systems currently used by the Post Office. New IT procurement frameworks established post Royal Mail separation, mean that the number of IT suppliers that Post Office currently uses could increase and therefore data sources could further fragment. Additionally, the added layer of an outsourced system integrator, could complicate the availability of data to the Post Office. The completion of the move to a new Data Centre platform for the major systems could be used by the Post Office to demonstrate that security considerations are being included in system designs and requirements. This will not mark the point at which systems are secure, but it will represent when gaps in systems are fixed.

7.5.1.3 Network Transformation Programme

As SPMRs are migrated onto the new Local and Main operating models remuneration packages the automatic payments under the old contracts will be removed. Although SPMRs minimum income will be guaranteed for the first 3 years, the Post Office will need a robust system to monitor transactional profiles over this grace period to ensure that SPMRs who are struggling financially do not undertake activity that artificially inflates their remuneration. Some SPMRs are also moving to a self-funding model, which needs to be closely monitored as there have already been some cases of loss/theft seen in this model.

7.5.1.4 Crown outsourcing complete

The completion of outsourcing of some loss making Crowns will represent an important milestone in the Post Office's evolution. The initiative has been difficult for the Post Office, with a determined campaign of industrial action. Once completed, the Post Office will be faced with ensuring the existing Crown branches become \ remain profitable and, that the new outsourced branches operate effectively. A key positive message to the network is a fit for purpose Process and Policy approach to ensure staff are treated fairly and that non-conformance is being addressed to reduce losses.

7.5.1.5 Cost neutral

To become cost neutral the Post Office will need to sell more profitable products and services. These are likely to be increasingly aimed at the financial services market. The

POL00004408

Security team will ultimately need to expand and expend more time on focussing on the threat of external fraud MOs.

7.5.2 Proposed transformation map for the security team

Figure 7-2 shows the proposed transformation map for the security team. The activities were identified with Post Office representatives along five work streams:

- Policy and processes;
- Technology;
- Data and Analytics;
- Central teams;
- Branch network.

7.5.2.1 Policy and processes

The activities identified here address the lack of consistency and shared understanding of security processes and policy as is apparent in the organisation. These are designed to first define and agree policies and processes across the core security teams, Fraud Analysis and Audit, and to deliver to training and associated change processes to embed the new approach in the organisation.

7.5.2.2 Technology

The technology work stream concentrates on both delivering new technology to the core security teams and inputting requirements into the re-design of the Post Office systems.

7.5.2.3 Data and analytics

These activities are focussed on improving access to and exploitation of data within the Post Office, including increasing the number of days of transaction data security teams have access to, improving the picture of branch activity and then starting work to access and exploit data on Post Office customers

7.5.2.4 Central teams

This work stream focuses on identifying ways to rationalise the proliferation of teams in the Post Office that do similar jobs but which work in silos. This rationalisation could not only save money but substantially enhance working practices and the management of branches

7.5.2.5 Branch network

The branch network work stream is perhaps, after the policy and process work stream, the most important set of activities, aiming to improve the engagement with staff and SPMR in the branch network. Changing their behaviour and improving their experience of working for the Post Office will reap large benefits, both in terms of improving security and customer satisfaction.

POL00004408

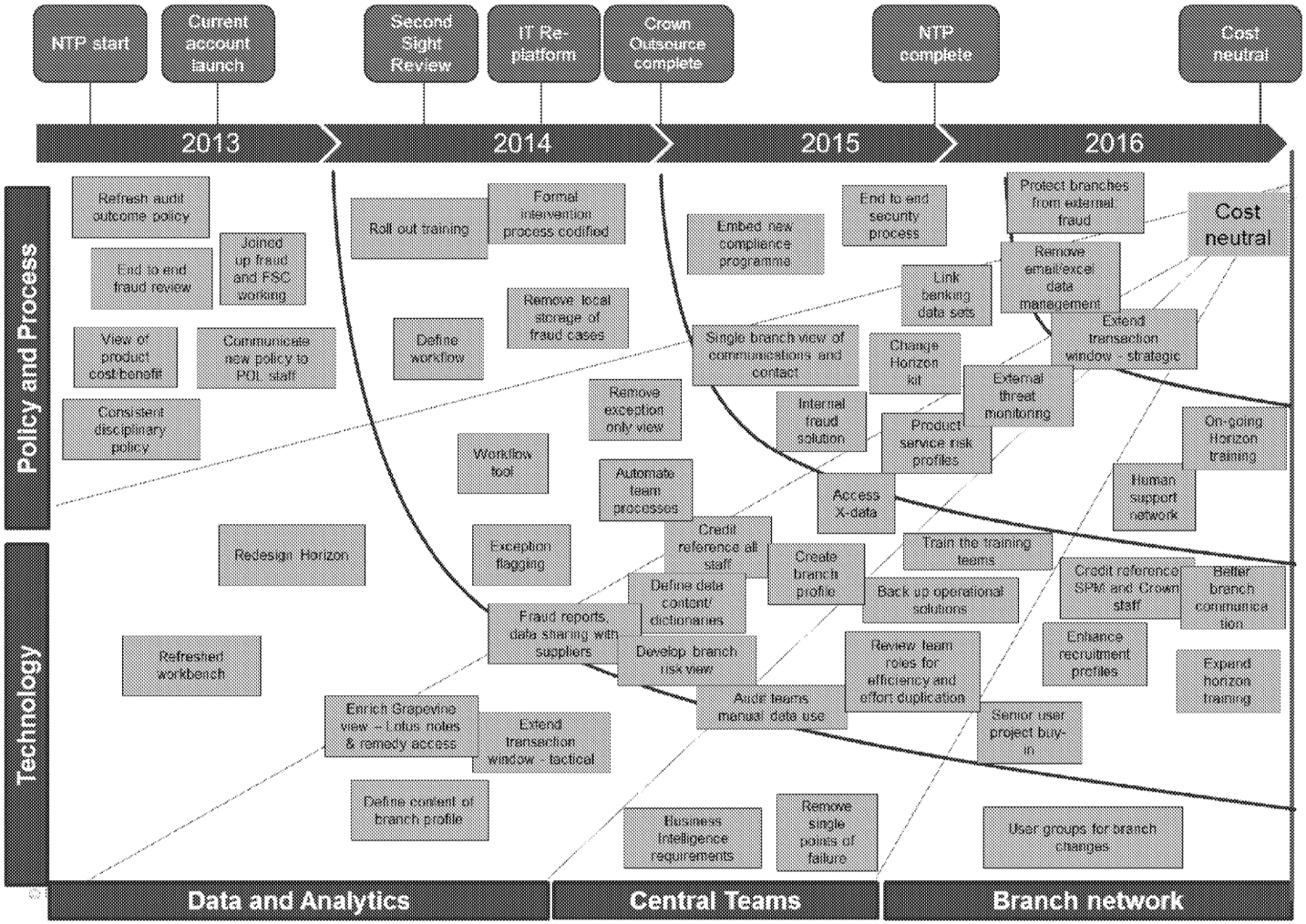


Figure 7-2: Proposed transformation map for Security road map; the blue boxes identifies activities which are currently in the process of being addressed; the green boxes represent activities which have yet to be progressed

POL00004408

A Data used in the Pilot

A.1 Data sources

The embedded spread sheet contains a list of all the data sources encountered during the Pilot

Data Sources used in Pilot 2013.xlsx

A.2 Data quality assessment

	Credence	HR SAP	Galaxy	Lotus Notes/ Electronic Filing Cabinet	Complaints	Flexible planning	ATM data
Reason for inclusion	Core transactional data set	Needed for Post Office employees	Required to monitor stock	Potential indicators of troubled behaviour	Required to indicate issues occurring in branch	Cash holdings in branch	Out payments of ATM to close cash exit loop
Definition	Unclear	Yes	Yes but in isolation of other systems	Yes	Yes	Yes	Yes
Accuracy	Transactional data yes, for concerns on reference data please refer to 'consistency'	There have been some concerns about the accuracy of what is contained with the system. Specifically some of the records Detica received indicated there were	Not used	Not available	Included in Analyzer for analysis, but content was not validated	Yes	Not accessed – there were some unconfirmed reports of their being concerns of the data being manually manipulated by the supplier.

POL00004408

		multiple of Sub-Postmasters in post simultaneously,					
Validity	Yes – mainly system generated values	Yes	Not assessed	Not available	Yes – simple data values	Yes – mainly system generated values	Yes – mainly system generated values
Integrity	Yes	Yes	Yes	Not available	Yes	Yes	Yes
Consistency	Concerns have been raised about the quality of the MDM data, which is the reference data. References to historic opening hours not being amended to reflect reality. Additionally Detica received 75 more start dates for Sub-Postmasters in Credence than in HR SAP.	Concerns have been raised about the quality of the MDM data, which is the reference data. References to historic opening hours not being amended to reflect reality. Additionally Detica received 75 more start dates for Sub-Postmasters in Credence than in HR SAP.	Whilst the data may be the same across systems, it cannot be interpreted as such as the codes that define stock units in Galaxy are not understood in the context of Horizon.	Not accessed	Centralised to one system only – some manipulation required to link Complaints to other data sources	Not accessed	No concerns have been raised
Completeness	The over writing of declared branch figures daily and only being able to access the data for 62 days limits this data.	There were approximately 150 branches where there was no start date for a Sub-Postmaster	Not used	Not available	Not accessed	Not accessed	Not accessed

POL00004408

Timeliness	The information entering the database is timely, however is summarised very quickly for analysis purposes.	The system is manually updated, and it has been suggested by some teams that this is not always completed in a timely fashion	It would appear that the system from a timing perspective is fit for purpose	It would appear that the system from a timing perspective is fit for purpose for the teams that currently use it	It would appear that the system from a timing perspective is fit for purpose	It would appear that the system from a timing perspective is fit for purpose	ATM data should be available with all other transaction data
Accessibility	Many teams do not have the access they require therefore spread sheets of downloads move from team to team, creating a challenging picture of what the truth is.	Limited – not easy to extract the data	It is limited to certain machines, and the internal mechanics are not fully understood	This system has seeming random access spread across the business but seemingly no owner	This system would be of use for the Security team, but they do not have access	Some of the constituting data would be of value to Security but is not currently directly accessible.	This should be directly accessed data stream to the Post Office.

Table 7-1: Data quality assessment of principal sources of data identified

POL00004408

B Key Risk indicators

The attached spread sheet contains a list of all the Key Risk Indicators identified during the Pilot and the ones which have been used in the modelling exercise.

KRI list for final report.xlsx

POL00004408

C Branch list and risk

The attached spread sheet contains the list of all branches included in section 5.3

Kohonen clusters.xlsx