POL00393731

POST OFFICE CONFIDENTIAL

Information Security Review

Post Office Limited

POca end-to-end Information Security, Technology and product process Risk Review

Document Details	
Author	Peter R Laycock (Infosec4business Ltd)
Owner	Willie Hughes - Client Relationship Manager POL Managed Service & Sourcing
Date of this document	13th February 2013
Version	1.1
Status	Final
Distribution	POL Information Security POL Security POL Managed Services POca Partners POca Client
Classification	POL Confidential
Document Retention Period	
Master copy of the document is stored in	
Last print date	

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

CONTENTS

[TOC \h \z \t "Heading 1,1,Heading 2,2"]

POL00393731

1 Glossary

Abbreviation	Definition
Account Number	The unique reference which identifies a POca account – made up from the 6 digit sort code and the 8 digit BACS account number.
ACF	Access Control Facility
ACT	Automated Credit Transfer
AFP	Advanced Function Presentation
AQA	Automatic Quality Assurance
AIS	Application Interface Specification
ASCII	American Standard Code for Information Interchange
ATM	Automatic Teller Machine
Back office	The team of HP personnel who work on queued work items, not interfacing real time with Cardholders – but may call out to cardholders
BACS	Bankers Automated Clearing System
BOB	Business Object Broker
BoI	Bank of Ireland
CBN	Child Benefit Number
Change Management Board	A body operating under a constitution that is responsible for reviewing and approving changes to the POca service, and keeping stakeholders (including Information Security) informed.
CICS	Customer Information Control System
CIP	Channel Interface Protocol
CIR	Committed Information Rate
CISP	Community Information Security Policy
CM	Configuration Management
CMS	Content Management System
COE	Common Office Environment
COTS	Commercial-Off-The-Shelf software packages
CPMS	Central Print Management System
CPT	Central Processing Team, responsible for supporting the POca account opening process
CPU	Central Processing Unit
CRM	Customer Relationship Management – sometimes also used to denote the software or user interface used by CSRs – as in, “the CRM interface” or “the CRM layer”.
CSR	Customer Service Representative works in Contact Centre, carrying out front office activities (taking calls from customers) and back office activities (letters and work queue items).
CSV	Comma Separated Values. A means of sending data in a text file with one record per line and each field in a line separated by a comma.
Customer	The POca cardholder; or otherwise customer of Post Office
DASD	Direct Access Storage Device – shared storage

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

Abbreviation	Definition
DBA	Database Administrator
DBMS	Database Management System
DDI	Direct Dial Interface
DES	Data Encryption Standard
Domain supplier	A partner organisation responsible for the systems and applications under its specific control and operation.
DP form	Direct Payment mandate form that enables funds to be paid into a POca account once opened
DPMS	Dynamic Print Management System
DR	Disaster Recovery
DRS	Data Reconciliation System
DSA	Data Staging Area
DWP	Department for Work and Pensions
EBT	Electronic Benefit Transfer
EVP	Extended Verification Process – a method of ensuring the customer is who they say they are by use of key personal questions and passwords known only to the customer – example "Mother's maiden name", "Memorable date". EVP also deemed to include signature in written correspondence
FAD	Financial Accounting Description – a code which identifies the PO branch
FI	Financial Institution
FPS	Faster Payments Service - UK clearing service that facilitates near-real time payment of low value instructions.
Front Office	The team of CSRs who handle the telephone interface with the POca cardholder
FTP	File Transfer Protocol
GD	Government Department
GUI	Graphical User Interface
HMRC	Her Majesty's Revenue and Customs
Horizon	The information system used to capture and process business transactions originating in Post Office branches.
HP	Hewlett Packard Ltd
IA	Input Accel
ICR	Intelligent Character Recognition (scanner reads handwriting and produces data output)
IDM	Integrated Document Management
IEC	International Engineering Council
IFN	Image File Number
I/O	Input/Output
IOS	Internet Operating System
Information security	The preservation of confidentiality, integrity and availability of information:

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

Abbreviation	Definition
	• **Confidentiality:** ensuring that information is accessible only to those authorised to have access. • **Integrity**: safeguarding the accuracy and completeness of information and processing methods. Integrity controls include those used to protect against fraud and those, which ensure the accountability of individuals. • **Availability**: ensuring that authorised users have access to information and associated assets when required
IPACS	Integrated Performance Analysis of Computer Systems
IP	Internet Protocol
IPT	IP Telephony
ISDN	Integrated Services Digital Network - a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media.
ISO	International Standard Organisation
ITSO	Information Technology Security Officer
IVR	Integrated Voice Recognition
LAN	Local Area Network
LINK LIS5	The specification that defines the communication methods and messages between Banking hosts and LINK
MI	Management Information
MIPS	Million Instructions Per Second
MIS	Management Information System
MOM	Microsoft Operations Manager
MQ Series	IBM's platform independent messaging system
NAS	Network Application Storage device
NAT	Network Address Translation
NBX	Network Banking Exchange (system managed by Fujitsu on behalf of POL)
NBSC	Network Business Support Centre
NIC	Network Interface Card
NINO	National Insurance Number
OCR	Optical Character Recognition (scanner reads typewritten information and produces data output)
ODBC	Open Database Connectivity. This is a widely accepted application programming interface (API) for database access. It is based on the Call-Level Interface (CLI) specifications from X/Open and ISO/IEC for database APIs and uses Structured Query Language (SQL) as its database access language
OEM	Oracle Enterprise Manager
OMON	Omegamon IBM OS 390 monitoring tool
OMR	Optical Mark Recognition (scanner reads checkboxes, tick boxes and barcodes and produces data output)

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

Abbreviation	Definition
Openlink	An implementation of ODBC
OSSG	Output Support Services Group
PAD	Post Office Authorisation Document
PAF	Postal Address file
PAN	Primary Account Number – the bulk of the long number shown on the front of plastic cards, indicates the issuer.
PAT14	A basic bank account specifically aimed at the "unbanked" based upon Policy Action Team report "Access to Financial Services"
PED	Physical Environment Definition
PI	Processing Interface (EBT connection to NBX banking system)
PIN	Personal Identification Number – a 4 digit number known only to the cardholder
POca:	The Post Office Card Account Management service including, but not limited to: • Interconnection to the Branch Network via the Horizon System • Interconnection with the POca Banking System. • The document scanning and image storage service. • The document management system and its fulfilment centre. • The Customer Management System. • Post Office Limited POca control team for management information • The Secure Electronic Online Communications System (SEOCS) • The Bank of Ireland ATM Network.
POca Risk Management Committee	The Risk Management Committee is the primary body for administering the Security Framework (or ISMS). This is a constitutional requirement of the framework and must meet at least quarterly. Post Office Ltd and POca service providers must be represented on the body; customer organisations who subscribe to POca services may also be invited to attend on occasion. Both the SIRO and ITSO must be represented at all meetings.
Post Office branch	A location where POca services are offered. It includes directly managed branches, franchised branches and sub-post offices.
PPA	Pre-populated Application
PPI	Printed Postage Impression
PUN	Pick-Up Notice – the letter sent to a POca account holder indicating his/her card is ready for collection at the PO Branch.
QAS	Quality Assurance System
RAID	Redundant Array of Independent Disk
RDF	Remote Database Facility
Risk assessment	Assessment of threats to, impacts on and vulnerabilities of information and information processing facilities and the likelihood of their occurrence.
Risk management	The process of identifying, controlling and minimising or eliminating security risks that may affect information systems, for an acceptable cost.
SAN	Storage Area Network

POL00393731

Abbreviation	Definition
SEOCS	The Secure Electronic Online Communication System used to provide two way interconnection to Government Departments.
SDC	Service Delivery Centre
SIRO	Senior Information Risk Officer
SMC	Service Management Centre
SOAP	Simple Object Access Protocol – SOAP is an XML based lightweight protocol for exchange of information in a distributed environment.
SSH	Secure Shell
Stateless	A computer process which has no partial results or residual data which endures beyond a transaction boundary. In practical terms it means the system has no data which needs to be backed up.
SWIFT	Society for Worldwide Interbank Financial Telecommunication – a financial messaging network which exchanges messages between banks and financial institutions.
TACL	Tandem Advanced Command Language
TCP/IP	Transmission Control Protocol / Internet Protocol
TCT	Thames Card Technologies
TDP	Tower Document Portal
TED	Technical Environment Definition.
Third party	An individual or organisation that is neither: • A domain supplier employee or contractor involved in POca delivery, nor • A Post Office employee or contractor.
TIS	Technical Interface Specification
TIFF	Tagged Image File Format
TMF	Transaction Monitoring Facility
VPN	Virtual Private Network
VSAM	Virtual Storage Access Method
WAN	Wide Area Network
XML	Extensible Markup Language

2 Purpose of the Report

Post Office Limited Information Security department has adopted the International Standard ISO27001:2005 Code of Practice (formerly BS7799) for Information Security Management as the primary reference for designing and implementing information security. Use of the standard enables Post Office Limited to deploy security controls consistently across all business units and to define its requirements for security in all third party contracts, joint ventures and partnerships. The standard also provides a means of benchmarking against other organisations and a method of checking that security polices and standards are being implemented effectively. In addition to Information Security the risk review process and methodology also looks

POL00393731

for opportunities to improve customer experience, service levels and minimise fraudulent opportunities

3 Introduction

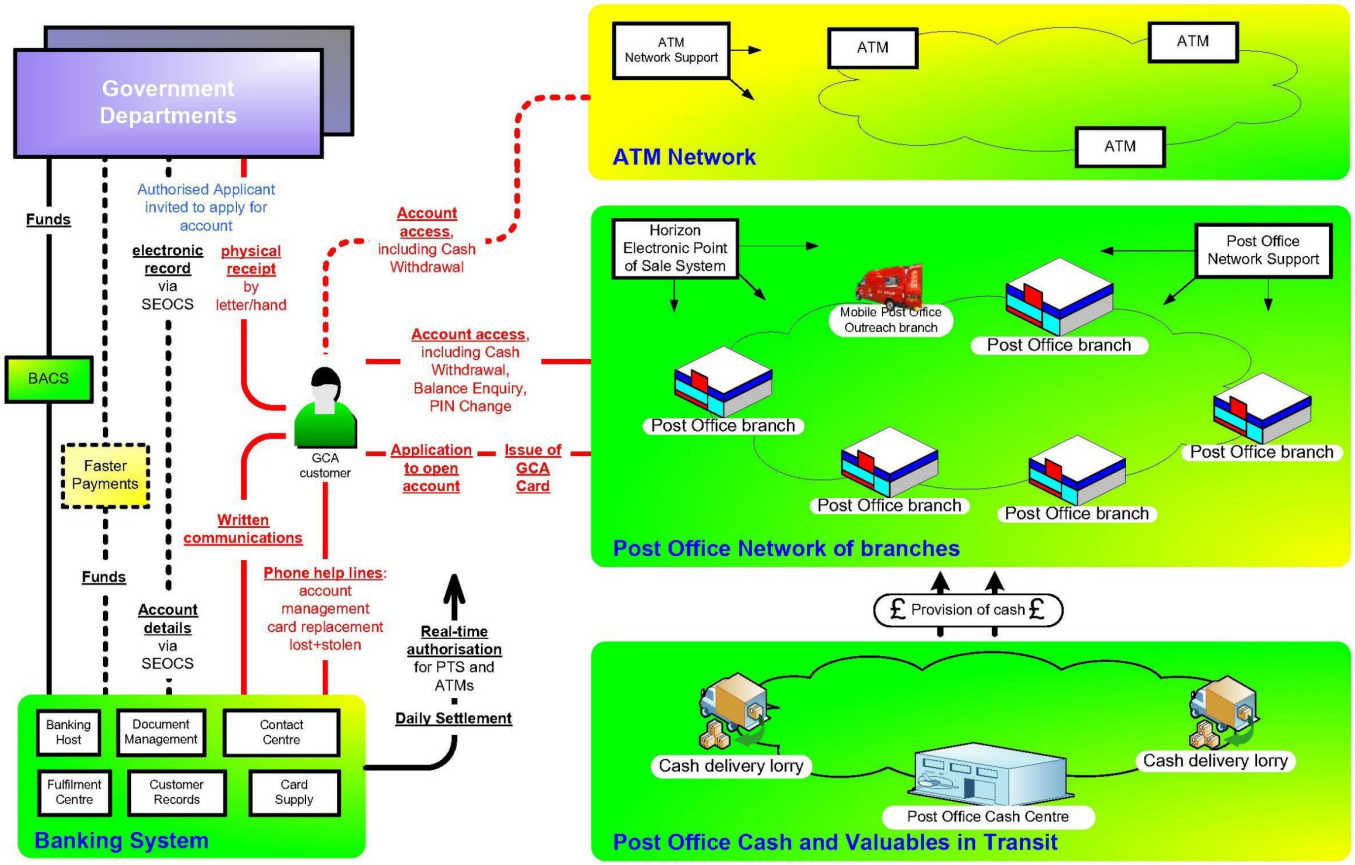
The Post Office Card Account was introduced in 2003 as a replacement to the Order Book system. Benefit and tax credit claimants were offered the POca if they did not have, did not want, or could not open an account with a High Street Bank. In 2009, Post Office limited was awarded the extension to the contract, which runs until 2015.

The product is operated by Post Office Limited on behalf of the (DWP) Department of Work and Pensions. Post Office has sub-contracted all customer management processes and technologies from their partner HPES (Hewlett Packard Enterprise Services) who in turn have a contract in place for the Banking Licence and EBT (Electronic Benefit Transfer system) element with JP Morgan Europe Limited.

POL00393731

4 POca Environment diagram: Overview

N.B: For GCA customer read POca Account Holder



POL00393731

5 Background

As agreed in the POca Security Plan (embedded at the end of this document), Post Office Limited will undertake an Information Security Risk Review every two years.

The objective of the Information Security Risk Review process is to examine the people (roles), processes and technologies required to deliver the POca product from initial invitation and application processing through account opening, use at the counter, account servicing by telephone and paper through to closure or dormancy, with the specific brief of protecting customer personal data, operational continuity, the brand image and stakeholder confidence of Post Office Limited, the Authority, and its partner organisations.

The review process investigates the controls in place, which are designed to protect against malicious or accidental loss of Confidentiality, Integrity and/or Availability of customer personal data, and/or customer financial information. The review also looks at areas where fraud might be committed (or has been) in order to minimise the possibility by recommending service improvements. In addition, particular attention will be paid to areas where incidents have been reported to ensure that root causes have been addressed to minimise repeats.

Although the primary purpose of the review is Information Security, Fraud minimisation and Data Protection, additional value has been added by also looking at areas where it might be possible to minimise application (and other forms) rejection rate, to improve customer experience and minimise adverse effect on agreed Service Levels.

As agreed in the original terms of reference for the Information Security Risk Review, the consultant uses meetings, workshops, observation and interviews with users, super-users, customer service representatives, managers, business operations staff, IT specialists, and administrators of processes and Information Systems, making use of ISO17799: 2005, Information Security Code of Practice, together with ITIL Service Management Standards, in order to produce a narrative based report of risks and additional or enhanced control recommendations.

Identified risks and recommendations for mitigating controls will be summarised in an associated risk action/treatment plan which will be a living document showing ownership by organisation and if agreed individual; actions against risks, through to details of compensating controls, acceptance of risk or mitigation and closure. New risks will be added to this document as the threat landscape changes but won't necessarily be reflected in this report document, which reflects the status of the product delivery at the time of publication

POL00393731

Important note: The PAD issuance process is part of the end-to-end POca process but within the Authority's domain. The authority's people, processes and technologies are out of scope of this review, but the initial process is described at a high level, together with risks previously highlighted following SEOCS service outages.

6 Overall POca Service Impact Assessment

The POca Account Management System has been formally assessed by Post Office Limited as part of their risk management process as follows:

SUMMARY OF SECURITY IMPACT CLASSIFICATION

Security Aspect	Security Impact Classification			
Business Criticality	CRITICAL	_	_	_
Confidentiality Overall Rating	CRITICAL	_	_	_
Confidentiality Maximum Score	CRITICAL	_	_	_
Integrity Overall Rating	_	HIGH	_	_
Integrity Maximum Score	CRITICAL	_	_	_
1 hour Availability	CRITICAL	_	_	_
4 hours Availability	CRITICAL	_	_	_
1 day Availability	CRITICAL	_	_	_
2 Days Availability	CRITICAL	_	_	_
1 week Availability	CRITICAL	_	_	_
1 month Availability	CRITICAL	_	_	_

Information which may specifically identify a POca account customer has been formally classified as Post Office CONFIDENTIAL. All other information has been classified as Post Office INTERNAL.

POL00393731

7 Management Summary

Some high-level overview information in this report is taken from existing HP technical documents with their permission

Particular thanks goes to Mark Geldart of HPES who has accompanied the consultant during all onsite reviews of people, processes and technologies within the HP and JP Morgan domains, ensured that all protocols were followed and assisted in a thorough review.

It is important to remember that the POca product is aimed at UK citizens who are in receipt of government benefits but who do not have, do not want, or in some case cannot have a bank account. The customer demographic has been referred to as "financially excluded" and "unbanked", but it is vitally important that DWP, Post Office, and its delivery partners does not lose sight of the fact that many POca customers are vulnerable, with physical and learning difficulties. Many are aging and although were quite capable of managing a simple financial product at the time of application time is taking its toll. UK citizens are living longer but not necessarily as cognitively capable as they age. Both PO Counters and the HP POca Contact Centre are experiencing more and more that many aging customers are struggling to enter a 4-digit PIN, and to successfully authenticate themselves over the phone by means of "memorable" information. It is not only Post Office that is having to manage these issues, but many other UK financial institutions and banks are also.
Note that this issue has been recognised by other banks and the UK Payments Council commissioned report is linked here:

[HYPERLINK "http://www.paymentscouncil.org.uk/files/payments_council/payments_council_-_policis_and_toynbee_hall_older_old_and_disability_report_24.10.12_final.pdf"]

The review has been very thorough and not in the style of an IT audit which in essence is a check that protective controls are in place. The benefit of the methodology used is that high risk processes are walked through with those performing the actual job. This not only enables the consultant to identify areas of vulnerability, missing or inadequate controls, but also enables improvement recommendations which benefit the product delivery and customer experience.

This method of review also highlighted the discovery of the one CRITICAL risk (Section 21.3) during the data centre visits for which immediate steps were introduced to mitigate, with further process revision still under discussion at the time of publication. Moreover, this discovery also provides some evidence that the major incident, reported in October 2012, would have been identified had events not overtaken the review

POL00393731

Thanks go to all those who contributed to the review, some of whom were present during quite lengthy meetings and onsite visits

At a very high level what can be said unequivocally is that everyone in every partner organisation which has contributed to this exercise has been open, honest and supportive. Each organisation of course wants to deliver a secure, successful and robust product, and on the whole it is.

If one message can be taken from the exercise it is this*: it is not possible to fully de-risk the possibility of incident or data loss/compromise as long as databases are unencrypted at rest, and that paper output is required, which is delivered by machine with operator management. Where there are machines, there will always be faults, where there are people there will always be a level of risk. We can make things better and learn from mistakes but never can we make things perfect.*

7.1 Department of Work and Pensions and HMRC (PAD issuance and transfer)

It should be noted that although dialogue was had, the DWP did not wish the Consultant to review the production of PAD records in a sample Job Centre Plus, nor follow data into the DWP Enterprise Business Gateway at the Norcross Data Centre through the SEOCS infrastructure. We must bear in mind though that a planned power outage at the DWP Norcross Data Centre over the 2011 Easter holiday resulted in missing PAD records. A root cause analysis (RCA) was received and critiqued, but this pointed to the fact that there are risks to service availability. In the absence of evidence to the contrary, it is assumed that the same risks still apply today, which are:

- The E-Business Gateway appears to be a single-point-of-failure in relation to POca
- The Norcross Data Centre appears to be a single-point-of-failure in relation to POca
- PAD File deletion is performed purely on the passage of time (5 days) and not on success criteria as would be best practice
- Phishing and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**. This attack led to RSA having to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain.

POL00393731

- The HMRC incident (August 2012) where loss of the PGP Desktop encryption software on their desktop PC caused the failure to transmit tax credit customer PAD records for seven working days. This highlighted the fact that the sending PC in the HMRC domain is a single-point-of-failure.

7.2 Post Office Counters

It was not possible to view any POca paper transactions (e.g. applications or other forms check and send) during counter visits in that none appeared during the visits. However, during the visit to HP Swansea Input Capture Centre the receipt and processing of forms was fully witnessed which enabled the Consultant to identify issues and areas of possible improvement.

7.2.1 Fraud issues and improvement recommendations

- Grapevine [HYPERLINK "https://www.grapevine.co.uk/Section/About"] is not widely known about in the Post Office Branch network. An event just after the Consultant left a branch occurred. An old lady took £600 form her POca, and placed the money in her shopping trolley. A young woman was sitting in branch seemingly waiting for someone, but suspicions were aroused when she followed the old lady out. Branch Manager and clerk follow just in time to see woman engage old lady with "that's a nice shopping trolley, a bit like my gran's". Branch staff arrives just as the young woman is trying to steal the money. She runs off. Staff informs local shops and Arndale Centre security but the woman's description and indeed CCTV image would have been an opportunity to use Grapevine for such events. The role and benefits of Grapevine and a national intelligence database are not widely known in the Crown network. An awareness campaign may bear fruit.
- Overuse of "withdraw limit" transaction. Nearly 70% of all cash withdrawal transactions committed at the counter are the "withdraw limit". The lack of customer sight of the transaction value is a facilitator for fraud, and at periods when additional deposits have been made into the POca (e.g. Winter fuel or double pension at long Bank Holiday) customers are often surprised at the amount of money they receive
- Customers should be encouraged to always insist on a receipt for their transactions. Where counter fraud is perpetrated in general the customer has not been given a receipt, or provided with another from someone else's transaction. A small, but bold and prominent notice at every counter position will help
- Where POca fraud has occurred, some cases have resulted in prosecution and prison for offenders. Courts take very seriously fraud perpetrated against the old and vulnerable. Publicity of these prosecutions in Counter specific publications and articles may act as a deterrent
- Some POca customers struggle with PIN pads, and whereas we tend to assume that entering a 4-digit PIN is not difficult, for some of the POca demographic

POL00393731

it very much is. Although strictly against instructions, and a breach of POca customer terms and conditions, some outlets are helping customers enter their PIN. Whilst admirable that staff assist struggling customers, entering a PIN for them opens staff up to accusations of misuse, and indeed court cases have proven that some rogue staff have taken advantage. Struggling POca customers should be advised to appoint a Permanent Agent. If the POca customer does not have a trusted friend or relative, we should be asking the question "Is POca the right product for all"? Should we be asking customer to contact paying agency to provide advice on alternate methods of payment? Could the "contactless" functionality on the new Ingenico PIN Pads be used to provide an easier method of doing business for the less able-bodied?

- P6167 Account Closure process does not require EVP authentication, or face-to-face identity check. POca can be closed and all residual funds transferred by cheque or transfer purely on signature validation. This process is known to have been misused. The perpetrator was sentenced to 6 months. See body of report for improvement recommendations
- Phishing and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**. This attack led to RSA having to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain.

7.2.2 *POca (and other banking transaction) mis-keys*

- Mis-keys at the counter for banking transactions is still a major issue, impacting agents, and taking up much P&BA resource to manage in relation to compensating transactions with partners banks. The vast majority are of course accidental, but deliberate mis-keying of cash transaction values can be to the benefit of criminally minded customers, outlets or clerks (or a conspiratorial combination thereof). The consultant made the recommendation that Post Office should consider **double entry and cross validation of free form banking transaction values (withdrawal and deposit)** in his report dated July 15, 2008. This recommendation still stands. It should be noted that doing so will not impact queuing time, and will indeed save time in that management of mis-keys as they happen does impact the queue. Many other products will benefit if this control is considered for all monetary vales entered on Horizon (i.e. values not created by reference data). The author has been recently consulted by the "mis-keying" project.

POL00393731

7.2.3 POca forms errors affecting reject rate and customer experience

- Common errors during form(s) checking at the counter which lead to rejection back to customer or SLA impact:
    - P6629 (application form):
        - FAD Code missing
        - Date mismatch between date stamp and written date
        - Outlets hanging onto forms rather than sending after each working day (except Saturday)
    - P6363 (evidence of ID form):
        - Two items of ID recorded where one will suffice and one entered incorrectly
        - ID Item number not recorded
        - Birth certificates provided as ID when married women's names have changed
        - Customer names entered incorrectly on form creating mismatch with application
        - Failure to send P6363
    - P6164 (deceased account form):
        - This form requires a representative signature and, if there is a balance on the account, an indemnifier signature. The latter is often missing, resulting in rejection of the form back to the informant, but at the address of the Primary Account Holder, who is of course deceased. This causes unnecessary distress. Note that the Horizon Help screen indicates that the form does not always require Section 4 completing. This is wrong.

7.3 HP Swansea Input Capture Centre

The work performed in the HP Swansea Input Capture Centre is receipt, sorting, batching, scanning, secure storage, recovery on demand, and secure destruction of each and every POca document sent from Post Office outlets. Rejection letters are sent from Swansea back to the customer with forms which contain errors or where the identity check has not been to the required standard.

It should be noted that although the work is particularly boring, repetitive and simplistic, it is vitally important that every document is accounted for and retrievable as a scanned image, and that returns to customers are accurate in terms of envelope contents.

As far as is possible, a flexible working approach is provided for staff, some of whom are agency employed and others on HP contracts. Leigh Gough, the Centre Manager

POL00393731

ensures as far as possible, that the POca product benefits from a content and happy workforce who understand that accuracy and data protection are paramount. All staff are vetted to agreed standards and there is a low turnover. Even in low paid positions, treating staff fairly engenders a certain element of loyalty, which leads to better care in terms of service quality

There has been one event reported which could have become a Data Protection incident due to an error in Swansea, which initially indicated that documents for rejection may have been returned to the wrong customer. It was later discovered through customer contact that the only issue was that a P6363 (Evidence of Identity) document was sent to a customer in error. The Consultant is satisfied that additional controls have been put in place to minimise recurrence. It must be borne in mind however, that the process for rejection and envelope stuffing is manual and therefore always subject to human interaction.

7.3.1 Risks identified in Swansea Input Capture Centre

It should be noted that since the Consultant's previous visit and Risk Review many improvements have been made, and all previously identified risks adequately controlled. Only two areas were identified, both of which were agreed by HP and both of which are being mitigated:

- Keys for the locked boxes, which contain POca forms and associated correspondence for secure waste disposal, are held by building Facilities Management Company, ISS. This means that in theory documents could be compromised out of hours without discovery. These keys will now be brought back into HP control (Leigh Gough's locked key cabinet in his locked office) to minimise any possibility of misuse.
- John Cavell is the technical expert for the Input Accell document scanning system. John could be possible single-point-of-failure should anything untoward happen to him. However, HP has recognised this risk and is ensuring that knowledge is shared
- Phishing and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**. This attack led to RSA having to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain.

POL00393731

7.4 HP Preston Contact Centre

The POca Contact Centre is located in Preston town centre and provides all account servicing capability whereby customers who call GRO will be greeted by a fully vetted and trained Customer Service Representatives (CSR) who are a mixture of Kelly Services Agency staff and HP employees.

CSR's are recruited by Kelly Services and following a 2-week intensive training programme become a "Tier 1" CSR. The training agenda is embedded in the control summary below: Some of these CSR's are taken on as permanent HP employees into Tier 2, Case Management and other more senior roles. It should be noted that the ability for CSR's to benefit from career progression engenders good employer/employee relations and minimises the chances that staff will look for opportunities and process gaps that might be exploited for personal gain. The Consultant did a similar review of the Contact Centre in 2007 and stated in his report "Low pay and lack of secure employment can lead to an increased risk of accidental or criminal misuse of available information, in that there can be more to gain than to lose".

The review in 2007 came on the back of two particular frauds where advantage was taken by two or three agency staff that utilised a lack of transaction segregation in the lost/stolen process and the P6167 account closure process to steal from POca accounts. Both resulted in prosecutions. It must be said that likelihood of CSR misuse is less now than previously in that controls recommended by the Consultant previously in terms of duties segregation and desktop lockdown have been implemented. Also, employment rights for agency staff tend to mirror those of substantive roles and career progression is very much in evidence.

It should also be noted also that Post Office has redesigned and passed over the POca Claims and Disputes process which is being run well by the Contact Centre Case Management team. More recently some security investigations work, liaison with Police, and completion of Witness Statements has also been passed over to HP.

On the whole, from the observations made in the Contact Centre during this review, the impression was one of well-managed, well-motivated and loyal workforces who take a great pride in their work and recognise the sensitivity of their role in terms of customer interaction. It should be noted that some customer calls can be particularly difficult but are on the whole managed with courtesy, compassion and professionalism by staff who understand the need for sensitivity and security.

7.4.1 Risks identified in Preston Contact Centre

- Different telephony losses at different times result in the invocation of different call plans. Call Plan F has been troublesome in the past. It is recommended that a rehearsal of Call Plan F be agreed to ensure that all from

POL00393731

HP, POL and BT are aware who needs to do what, when and why. All other Call Plans invocations should be similarly rehearsed to ensure they are fit for purpose.

- Although each component of the POca end-to-end is rehearsed annually to ensure that recovery following a disaster is doable, this does not prove every process. For instance, we have never done a full rehearsal of SEOCS paper fallback in that it was very resource hungry, although now we have agreed a secure and simple process for SEOCS outage by copying PAD records encrypted discs. Nor have we simulated though the loss of the link between HNG and EBT for instance, and the requirement to provide emergency payments and in the case of total service loss, provide emergency payments and hold on to the card in branch. It is therefore recommended that the emergency payment processes be reviewed and also that a Crisis Management exercise is planned which simulates specific scenarios which may not be catered for in a DR test
- Handoff from Tier 1 CSR to Tier 2 CSR can be problematic if Tier 2 are engaged. This handoff isn't automated so Tier 1 CSR must try each in turn but often get the response "I'm not available as Tier 2". This can result in a poor experience for the customer who is on hold.
- There are certain transactions which can only be performed EVP levels 1 and 2. E.g. PIN Unblock, Large Cash Withdrawal or Partial Balance Release by cheque. In addition it has recently been agreed that for LCW and PBR only Tier 2 and greater will be allowed to authorise. During the Consultant's visit Tier 2 were asking "has the customer passed EVP?", whereas I would have hoped the question should have been "At what level did the customer pass EVP?" Better still would be that Tier 2 will take the customer through EVP.
- Customer statement requests are handed off to Tier 2, but there is no obvious reason why this process could not be performed by Tier 1. It seems to require only that a form be populated with from and to dates.
- There seems to be three different processes for cheque issuance for a POca. A partial balance release can be requested by phone will initiate a cheque in x days; a written request for a cheque will initiate a cheque in x days. But, there seems to be a third and much slower process which the Consultant heard during a call from a prisoner. The prison governor had given authority for the residual balance of the prisoner's POca to be paid by cheque to the prison – in the name of the Governor, yet the prisoner was told that it may take 28 days. This process should be reviewed.
- There may be a fault with PEGA in that when the Tier 2 CSR was showing a screen from an account with lots of account activity the screen went black. The CSR said that this only happens when there is loss of activity recorded.
- Case Management team are still receiving some emails from POL Security investigators which are not encrypted. Any and all communications from POL Security to HP should be routed through POL Security Support team in Salford Quays and be protected by PGP.

POL00393731

- Requests by Police and DWP Fraud for copies of customer personal information is acceptable under Section 29 of DPA 1998 if the request is being made for Criminal or taxation purposes. That said, it is recommended that a watermark be added to every document to the effect that the recipient is responsible under DPA to protect the information and securely destroy when the need has expired.
- The Contact Centre Operations team have very good processes, one of which is the ability to keep a track of every event in the career of a CSR. E.g. when access levels were granted, suspended, revoked, or enhanced; role changes; dates of maternity leave etc. etc. This is not the case though for all HP staff working on POca. It would be useful to share this best practice; particularly for IT systems and database managers.
- The "gone away" process is where correspondence is returned to sender. This process, in conjunction with the P6167 has been misused in the past for personal gain. Although probably less likely, it would still be possible today. There are other control recommendations in this report but the following should be also be considered by HP: Remove account details from CSR screen when investigating "gone aways"
- Phishing and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**. This attack led to RSA having to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain.

POL00393731

7.5 HP Washington Fulfilment Centre

The visit to Washington Fulfilment Centre was very productive in that the operations staff kept back a full batch of statements which the consultant could witness from file receipt through printing, stacking, stuffing, enveloping to following through the mailing process to the secure dock where Royal Mail vans arrive.

Thanks go to all those involved. The batch in question was 5,864 statements. Although successfully completed it was noticeable that problems with stacking to the perforations was somewhat difficult and the hopper of the printer used might be past its prime. During stuffing and enveloping there were some 22 jams, which may have been more than was usual and all of which were managed, but a contributory cause may have been the poor stacking after printing.

There have been incidents reported to Post Office when a very small number of customers have received statement pages belonging to others with their own, which has in the past been put down to machine error, dirty OMR sensors, and also human error by not following due process for jam management. That said, Washington prints some 13million statements per annum plus all other letters, PUNS, PPA's and PIN mailers so the percentage wrong is infinitesimal. That said, any error which causes customer A to receive the personal information of customer B is a Data Protection incident and is treated very seriously but we must bear in mind that the five incidents which have happened in the past year is in actuality a success rate of 99.99996. To put this into perspective, the risk that the Royal Mail will deliver a statement to the wrong home is far greater. We can always make recommendations for improvement as have been made in this report, but de-risking a mechanical process with manual control is not possible

At present statements are sent out quarterly, but a change has been approved and budgeted for to change this frequency to 6-monthly as the default whilst giving customers the ability to choose quarterly or monthly. It was obvious during the witnessing that problems do occur when envelopes are stuffed with more than 12 sheets. Once the change is introduced, the likelihood of hitting this 12 page limit is high. HP has said that this has been catered for in the design process but is documented as a risk in this report until such time as the change is implemented and the capability to stuff more than twelve is proven

Whilst witnessing jam management it was noticed that all spoils are spread on a table to manage when the batch is finished. It seems that this scattered approach may increase the risk of error so a risk and recommendation is made below

POL00393731

8 JP Morgan (Europe) Limited

Thanks go to the staff of JP Morgan (Europe) Limited for their time, expertise, honesty and openness during two lengthy workshop sessions. JP Morgan's (EBT) Electronic Benefit Transfer service delivers the back-end banking service which interfaces with POL Horizon, Vocalink ATM network, and HPES CRM service.

The EBT service is delivered from HP Doxford Data Centre with DR in the HP Wynyard Data Centre. The technology is based upon the banking industry tried and tested "[HYPERLINK "http://en.wikipedia.org/wiki/Tandem_Computers"]" system, which delivers a real-time, fault tolerant service with zero data loss. The tandem platform is tried, tested and trusted and used worldwide for financial, banking, military, air traffic control, USA hospitals etc., i.e. where High Availability and no data loss is of crucial importance.

Each and every process detailed in the POca lifecycle document was thoroughly reviewed by the Consultant with JP Morgan Production team, IT technicians and HP's Production Support/Security Manager. Low level details of each of these processes are embedded here:

POca steges with JP Morgan involvement.:

No major risks were identified in the JP Morgan arena, but there were some observations

Caveat: The application level review was performed in advance of the Data Centre infrastructure level review and prior to October 2011 when an incident was reported. This initiated a full review of the EBT hardware maintenance contract. The consultant has reported satisfaction with the new contractor and processes, notwithstanding some minor risks. That said, it is also recommended that a more targeted review of the EBT service is made to minimise the risk that any further incidents may occur. See Section 25.1 below and embedded report on recent changes to the EBT (Tandem) hardware maintenance contract

8.1 Risks identified in JP Morgan (Europe)

1. Following the October major incident which identified a "CRITICAL" risk, urgent changes to hardware maintenance work were introduced. This review was delayed at that time as the focus was on improvements necessary to

POL00393731

reduce the risk. The consultant performed a review following which some minor risks were outstanding and are detailed in the embedded report

2. JP Morgan (at the office level) benefits from robust controls against data loss, which includes full lockdown of USB and CD writing capability (except in authorised circumstances). Also, all attachments to emails are automatically checked. That said, the automated check may just ensure that attachments are encrypted. It might therefore be possible to send out an email attachment containing customer personal or corporate confidential data which has been encrypted, even if this contains information that should not leave the business
3. Phishing and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**. This attack led to RSA having to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain.

9 Government process for opening and sending PAD records

The following is the process used by Government departments for the opening of a POca with the claimant: Please note that numbering is their own. They haven't provided bullets 1 → 11.

9.1 The POca opening process

12. The POca opening process provides an on-line PAD to initiate the application process, replacing the Personal Invitation Document (PID). Business as usual activity requires that any contact with claimants about which Method of Payment (MoP) they would like to use must include a Method of Payment Policy discussion.

13. If the claimant requests a POca, you must consider the Exceptions (instances where a claimant cannot open a POca) and have the POca follow on conversation with the claimant face to face or over the telephone.

14. If the Method of Payment Policy discussion and POca follow on conversation has not taken place, then a PAD must not be completed.

POL00393731

15. If after conducting the POca follow on conversation the claimant does not wish to proceed with opening a POca, another MoP must be agreed. Use the MoP discussion.

16. If the claimant wishes to pursue their application, open and complete the PAD on-line during or after your discussion with the claimant as suits your local practice.

Note: Rather than open the PAD through a web address each time you need it, you can save the link to the PAD as an icon.

Note: If an appointee is applying for a POca then the PAD needs to show the claimant name and NINO but the rest of the PAD must be completed with the Appointee's details.

17. When the PAD is completed and checked, click on the 'Submit' button at the bottom of the form. This action will send the PAD details via CPTMS to POL.

` 18. On receipt of the PAD from CPTMS, POL will send a form (which is already populated with the claimant's name, address and expiry date) to the claimant for checking, completion and return.

19. POL consider the application, and if successful will separately post the claimant a Pick up Notice (PUN) and Personal Identification Number (PIN) asking the claimant to go to their chosen Post Office to collect and activate their POca card.

20. When the card is activated POL will send the account details via CPTMS to CPT who will input them to the relevant benefit system(s) each day.

21. From this point, benefit payments will be made into this account.

POL00393731

9.2 New Post Office card Account Opening Process Flow Chart

Claimant requests a POca

[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/a-z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20march%202010)/DWP_T508001-2.gif" * MERGEFORMATINET]

[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/a-z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20march%202010)/DWP_T508001-3.gif" * MERGEFORMATINET]

Does the claimant fall within the [HYPERLINK "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/a-z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20march%202010)/DWP_T508001-03.asp" \l "P37_5591"] Group – those claimants unable to open a POca?

[INCLUDEPICT "http://intralink.link2.gpn.gov.uk/1/j z/post%20office%20card%20account% 20(implemented%20from%208%20ma 8001-4.gif" * MERGEFORMATINE "http://intralink.link2.gpn.gov.uk/1/j z/post%20office%20card%20account% 20(implemented%20from%208%20ma 8001-5.gif" * MERGEFO

[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/a-z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20march%202010)/DWP_T508001-6.gif" * MERGEFORMATINET]

[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/a-z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20march%202010)/DWP_T508001-7.gif" * MERGEFORMATINET]

[INCLUDEPICT "http://intralink.link2.gpn.gov.uk/1/j z/post%20office%20card%20account% 20(implemented%20from%208%20ma 8001-9.gif" * MERGEFO [INCLUDEPICT "http://intralink.link2.gpn.gov.uk/1/j z/post%20office%20card%20account% 20(implemented%20from%208%20ma

POL00393731

8001-10.gif" * MERGEFO
[INCLUDEPICT
"http://intralink.link2.gpn.gov.uk/1/j
z/post%20office%20card%20account%
20(implemented%20from%208%20ma
8001-11.gif" * MERGEFO

Use the [HYPERLINK
"http://intralink.link2.gpn.gov.uk/1/corp/sites/finance/financialcontroldirectorate/guidance/dwp_s14909
discussion to establish with the claimant if another form of direct payment is available

POL writes to customer and sends [HYPERLINK "http://intralink.link2.gpn.gov.uk/1/jcp/guid
z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20marc
01-21.asp" \l "P457_38103"] and details to Shared Services Central Processing Team (CPT). Note: If cl
has a POca POL will write to customer and email account details to CPT who will change the claiman
payment. See [HYPERLINK "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_
z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20marc
01-21.asp" \l "P471_39119"] for Jobcentre Plus action.

[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/
z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20marc
01-18.gif" * MERGEFORMATINET]
[INCLUDEPICTURE "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_del/
z/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20marc
01-3.gif" * MERGEFORMATINET]

POL00393731

CPT emails [HYPERLINK "http://intralink.link2.gpn.gov.uk/1/jcp/guidance/bus_dz/post%20office%20card%20account%20opening%20process%20(implemented%20from%208%20marc 01-21.asp" \l "P457_38103"] and details to generic email address in owning BDC for any ac

POL00393731

10 HP Swansea Input Capture (control summary)

Also referred to as Content management System (CMS)

HP Input Capture Centre was reviewed by the Consultant in 2008 from which all identified risks documented at that time have been adequately and properly controlled.

It should be also noted that although the ISO27001:2005 ISMS (Information Security Management System) for POca does not currently cover the Swansea Input Capture Centre, the Swansea People. Processes and Technologies are being reviewed for conformance by HP, which will lead to a certification audit in May 2013, with the intention of certifying the site to ISO27001:2005

POL00393731

10.1 Solution overview

[SHAPE * MERGEFORMAT]

10.2 Control summary

The following list is indicative of the robust control provided as opposed to being exhaustive. Full protective controls will be detailed in the ISO27001: 2005 Statement of Applicability which will be kept by HPES, due to be audited and issued May 2013, and will be commercially confidential

- The building and all internal areas are protected from unauthorised entry by a swipe card system
- Use of mobile phones and cameras is strictly prohibited in areas where POca documentation is stored and processed
- Robust physical and logical access control and privilege management processes are in place enabling systems access to be provided and removed as needed
- All staff are vetted and undergo induction training and ongoing awareness of Data Protection requirements of roles
- All POca paper forms and customer correspondence are protected from unauthorised access (except for risk identified below)
- Input Accell scanning software benefits from expert development and change processes
- Development and test areas are distinct from live
- There are two Kodak Digital Science i4600 scanners providing the necessary resilience plus another at the DR site.
- All application and operating systems under full vendor support
- All desktop and server infrastructure benefit from ant-virus and security patching regime
- All desktops and laptops are protected by hard disc encryption and USB/CD lockdown
- Systems and infrastructure protected by firewalls
- Infrastructure fully resilient within the site
- Swansea Input capture processes (including 1 x Kodak Digital Science i4600 scanner, and IT systems are replicated and available at DR site
- The Swansea LAN is connected to the MPLS "cloud" to enable data to be sent securely to the Tower system at Preston and the DR Tower system at Doxford through an encrypted IPSec VPN. Note that all IT primary IT systems located in Preston are being migrated to Doxford with HP Wynyard hosting DR services.

POL00393731

Detailed specification of site, security, technology, people, processes and controls are contained in this embedded document: "POca Input Capture Physical Environment Definition". It should be noted that the PED documents are subject to change so should be seen as a snapshot at the time of this review.

POCA-0594 Input Capture PED v1 1.do

11 HP Washington Fulfilment Centre (control summary)

There are three primary fulfilment requirements for POca:

1. Printing of forms/letters/PIN mailers/Welcome Packs/PUNs
2. Card Production
3. Cheque production

Card Production is performed by Thames Card Technologies and contracted to HP, and Cheque is performed by Bottomline and contracted to JP Morgan, the latter being out of scope of this review, but it is recommended that cheque production should undergo the same level of scrutiny

11.1 Solution Overview

Printing requirements are fulfilled at HP's centre in Washington, Tyne and Wear. This facility is in a building owned by HMRC but leased to DWP. It was originally a DWP fulfilment centre but was "outsourced" to EDS (precursor to HP) some time ago

The Washington Fulfilment Centre therefore supports the POca service requirement for print, mail and despatch of all POca paper based output. It has a DR site at Norcross in Lancashire to cater for outage, which is annually proven by rehearsal as required by contract.

The following list is the paper based outputs for the product:

1. Welcome Packs
2. Pre-Printed Application Forms
3. Letters
4. Statements
5. Pick-up Notices (PUNs)
6. Personal Identification Numbers (PINs)
7. Welsh print

POL00393731

8. Large print
9. Invitation Pack

In addition to these paper based items, the Fulfilment centre is responsible for initiating delivery of Braille and Audio equivalents to POca customers. These are requested using the same workflow as the regular paper items but are sent to specialist external agencies to generate and dispatch the media types

Data files are provided in ASCII delimited format containing an overlay flag. Separate files for each output type are produced. Optical Mark Recognition (OMR) marks are included within the transmitted ASCII file.
Live data is retained for an appropriate period prior to despatch to enable resending to cater for spoils; when paper successfully despatched live files are deleted.

The same file information sent to printers is also transmitted to Tower for rendering and incorporating with the appropriate overlay so that the CSRs have an image of all outgoing mail

PIN Mailers are of course not rendered for viewing

11.2 Control summary

The following list is indicative of the robust control provided as opposed to being exhaustive. Full protective controls will be detailed in the ISO27001: 2005 Statement of Applicability which is kept by HPES and is commercially confidential

- Durham House: DWP building but unsigned
- Whole site accredited to ISO27001: 2005
- 24 x 7 x 365 security controlled entrance
- Swipe card entry
- Shared reception with DWP, and shared canteen but HP area zoned only for HP staff
- Phones and cameras prohibited (lockers provided)
- Print files are transmitted via encrypted network links using Connect:Direct
- All staff are vetted and undergo induction training and ongoing awareness of Data Protection requirements of roles
- Some agency staff are provided by Kelly but Kelly's contracted to perform same level of vetting
- New staff must identify themselves with passport or driving licence on day 1 before induction
- All levels of access provided on a job role basis
- Segregation of duties exists and no single individual can perform the full end-to-end process

POL00393731

- All application and operating systems under full vendor support
- All desktop and server infrastructure benefit from ant-virus and security patching regime
- All desktops and laptops are protected by hard disc encryption and USB/CD lockdown
- Systems and infrastructure protected by firewalls
- Infrastructure fully resilient within the site
- Generic logon to print only workflow so no risk of misuse
- Print runs are checked 5 times; 1st, last and 3 x random checks during. These checks are manual and made by checking that contents of envelopes are as they should be. This check does not of course apply to PIN Mailers
- Single operator manages whole of a stuffing/enveloping run to ensure continuity, accountability and management of spoils
- All spoils are put to secure bins with a van arriving at 6am every work day to shred onsite which is witnessed and signed for

12 HP Preston Contact Centre (control summary)

The following list is indicative of the robust control provided as opposed to being exhaustive. Full protective controls will be detailed in the ISO27001: 2005 Statement of Applicability which is kept by HPES and is commercially confidential

- POca customer management is certified to ISO27001:2005 (see embedded certificate
- The building and all internal areas are protected from unauthorised entry by a swipe card system
- Use of mobile phones and cameras is strictly prohibited in areas where POca documentation is stored an processed
- Robust physical and logical access control and privilege management processes in place enabling systems access and removal as needed. Leavers have all access removed on their leaving day
- Any CSR going AWOL, even for one day without notice has all system and swipe card access suspended
- All staff are vetted and undergo induction training and ongoing awareness of Data Protection requirements of roles
- All critical infrastructure is delivered from a well-managed and secure server room. Note though that POca systems, previously resident have been moved to the secure data centres
- The site benefit from uninterrupted power supply (UPS) and a diesel standby generator to cater for mains power loss or fluctuation
- All IT systems benefit from expert development and change processes
- Development and test areas are distinct from live

POL00393731

- All application and operating systems under full vendor support
- All desktop and server infrastructure benefit from ant-virus and security patching regime
- All desktops and laptops are protected by hard disc encryption and USB/CD lockdown
- Systems and infrastructure are protected by firewalls
- Infrastructure is fully resilient within the site
- No POca IT systems (except for SEOCS) have direct exposure to the public internet. SEOCS is protected by double encryption
- All POca data sent and received traverses the secure HP VPN
- Disaster Recovery following any given scenario from lost telephony through lost IT systems to lost building are properly planned and rehearsed for

12.1 CSR Training agenda

The following is copied from the HP CSR 2-week training agenda and illustrates the thoroughness of the training regime:

Week 1

Monday

- Welcome to HP
- Our Working Environment
- Security Awareness
- Card Account Awareness
- Government Agencies
- Overview Of JPM
- Money Laundering
- Call Centre KPI
- Listening to Live Calls
- End of Day Quiz
- Introduction to Account Opening

Tuesday

- Issues From Yesterday's Quiz
- Pega Overview
- Service Level Agreements
- System Security
- Disaster Recovery
- Communication Skills
- Listening to Live Calls
- End of Day Quiz
- Deceased Account Closure

Wednesday

POL00393731

- Issues From Yesterday's Quiz
- Complaints
- Recap Of Deceased Account Closure
- Introduction to Policies & Procedures
- Introduction to Pega
- Pega Practice
- End of Day Quiz
- Listening to Live Calls
- Issues From Yesterday's Quiz
- Account Opening & Tower Workshop
- All Points Bulletins
- Avaya Training
- Pega Practice
- Listening to Live Calls

Thursday

- Issues From Yesterday's Quiz
- Card / PIN workshop
- Kelly's Meeting
- Meet the Boss
- Introduction to P & P's Self Learning
- End of Day Quiz
- Listening to Live Calls

Friday

- Issues From Yesterday's Quiz
- Card / PIN workshop
- Kelly's Meeting
- Meet the Boss
- Introduction to P & P's Self Learning
- End of Day Quiz
- Listening to Live Calls

Week 2

Monday

- Issues from Friday's Test
- Communication Standards
- PEGA Practice
- General Practice
- Troubleshooting
- Practical Test
- Listening to Live Calls

Tuesday

- Final Written Test
- General Practice

POL00393731

- Feedback from Tests
- Meeting with TL, FTL, & Call Centre Manager
- Go Live with buddy

Wednesday

- Live with buddy

Thursday

- Live with buddy

Friday

- WESS Training
- End of training Kelly's catch up
- End of Training Trainer catch up
- Live with buddy
- Training Ends
- Handover to Call Centre

13 JP Morgan Europe Limited (control summary)

Note: since the date of the walkthrough of these processes and in advance of the physical onsite data centre review an incident occurred; this identified a gap in media replacement processes, and initiated a change of hardware support provider. A full report of the new service is embedded in Section 25.1 below

- EBT is based on the tried, tested and trusted [HYPERLINK "http://en.wikipedia.org/wiki/Tandem_Computers"] platform which provides high availability, non-stop, fault tolerant systems without data loss
- All POca data sent and received traverses a secure VPN, with no exposure to the public internet
- New account requests are subject to checking against Bank of England sanctions lists, and all accounts run against these lists on a monthly basis to ensure accounts are not opened for sanctioned people. The Bank of England can also make a request for accounts to be checked at any time
- The JP Morgan building(s) and all internal areas are protected from unauthorised entry by a swipe card system
- Robust logical access control and privilege management processes in place enabling systems access and removal as needed. Access control is linked to HR so allocation of rights is done on a job needs basis. A slick removal process exists and would also cater for emergency removal following disciplinary or dismissal
- The misuse or sharing or access credentials is a disciplinary offence, the sanction for which is immediate dismissal

POL00393731

- There are no remote diagnostic links or third-party access to the live system, only alert monitoring of the usual disc thresholds, memory and uptime by global systems monitoring teams on a follow-the-sun policy
- Application development, test and support services are provided by in-house dedicated teams**. There is no access to POca data from "offshore"**
- There are multiple levels of technician access to the different environments for development, test, QA, UAT etc. with a "break-glass" emergency process to cater for Severity 1 incidents. This process makes use of Enterprise Password Vault that provides full audit, authority and approval. Elevated passwords are time sensitive. This is an excellent process for emergency fixes
- Audit log files are not managed by or available to the same technicians who can make changes
- All data repairs are done via requests from the HP PEGA system, and are fully attributable to the repairer
- JP Morgan has a policy of "in-sourcing" so although contractors are used in service delivery and system support once proven tend to be offered full-time employment. This reduces risk of knowledge loss and reliance on people who may leave at short notice
- All staff are vetted and undergo induction training and ongoing awareness of Data Protection requirements of roles
- Staff have access to the public internet but some sites and functionality is restricted including, webmail, gambling, and file sharing sites etc.
- Remote access is possible over a VPN but entry to systems is via 2-factor token which provides one-time password generation
- Systems delivered from Doxford and Wynyard data centres which benefit from all expected availability controls including uninterrupted power supply (UPS) and a diesel standby generators
- All disc storage benefits from mirroring to minimise any data loss during disc failure
- The POca service is tested up to 240 transactions per second (TPS), which is double the average expected TPS
- All IT systems benefit from expert development and change processes
- Development, test, QA and UAT areas are separate and distinct from live
- The Tandem system core is generic and all global releases of code are taken but JP Morgan only activate the required modules
- No security patching for the Tandem system has ever been required, and of course the service is written in COBOL and does not have any connection to the world wide web so infections are very unlikely
- Expertise is available as needed in the support teams with adequate knowledge share to minimise any individual becoming a single-point-of-failure
- All POca data boarded onto EBT is automatically validated
- EBT data is subject to a very robust backup regime with all tapes fully encrypted and stored by Iron Mountain. Note that encryption of backup tapes commenced in 2010 so tapes required for retention purposes in advance of this

POL00393731

date and written in clear text. They are though all stored safely in Iron Mountain's facilities
- Tape recovery is proven annually
- All application and operating systems are under full vendor support
- All desktop and server infrastructure benefit from ant-virus and security patching regime
- All desktops and laptops are protected by hard disc encryption and Symantec endpoint protections which includes USB/CD lockdown, with a documented exception process on a job needs basis
- Systems and infrastructure are protected by firewalls
- POca delivery infrastructure is fully resilient
- EBT subscribes to Disaster Recovery and has a hot standby instance located in the HP Wynyard Data Centre

14 HP IT Systems

Note: since the date of the walkthrough of these systems and processes the physical onsite data centre review has been performed; this identified a gap in media replacement processes, and initiated the declaration of the CRITICAL risk detailed in Section 21.3 of this report

All HP POca IT systems are delivered from secure data centres located at Doxford and Wynyard, Tyne and Wear. The infrastructure, networks and environments are certified to the Information Security standard ISO27001:2005 and subject to repeat audit by external assessment to keep the certification current.

14.1 Generic protective controls

It should be noted that the POca HP IT systems, their use, the infrastructure, and the data centres in which they resides are part of the ISMS (Information Security Management System) certified to ISO27001:2005 which ensures that strict controls exist and are regularly proven to exist

The following list is indicative of the robust control provided as opposed to being exhaustive. Full protective controls will be detailed in the ISO27001: 2005 Statement of Applicability which is kept by HPES and is commercially confidential

- All PAD data is protected in transmission over the public internet by double encryption
- Tower access to POL users is protected by transmission encryption and strict access controls
- POL access to Tower is further limited to specific and agreed building sub-net IP address ranges
- POL access to Tower is limited to SLA data. i.e. POL staff do not have access to scanned applications or other forms/letters

POL00393731

- POca systems are only accessible to authenticated users over the HP POca VPN
- Staff with authorised access or support roles are vetted and CRB checked
- Permanent HP employees, as opposed to contractors, are used in the design, development or support of the services
- There are no remote diagnostic links into the POca services by any third-party support providers
- All systems are delivered from secure data centres at Doxford and Wynyard
- Data centres, components and networks benefit from n+1 resilience
- All operating systems, application, and database management software are in full vendor support
- Patch management is robust. All patches are fully tested and rolled out to other areas of the global HP estate in advance of POca systems which reduces risk
- Whilst service monitoring is performed from outside of the UK (Zaragoza, Spain) the ability to access POca data is not possible offshore
- Change control procedures are robust and include Post Office impacting and sign-off
- There are robust testing procedures through to UAT which minimises any problems or issues when migrating to live
- There are different test environments (Development, Test 1, Test 2, and UAT) which are separate from the live environment. SEOCS and Data Staging are exceptions to this but this was agreed by the project
- Test data is always fictitious. I.e. live data is not used for testing. The only exception to this was for migration testing to prove the recent centralisation project for which, with POL approval, live data was used with strict protective controls in place
- All infrastructure, servers, storage and network components are resilient. i.e. internal component failover and no single-points-of-failure; the two notable exception to this rule are the Data Staging server used to send a monthly copy of POca data to the POL Brands direct marketing database, and the link to POL for Tower access for MI purposes. Neither of these functions are deemed critical to the operation of the product so this was a business decision
- All data is backed up and recoverable at a given point in time if needed
- All backup tapes once written are secured offsite by Iron Mountain
- Regular service review meetings are held to where incidents are reviewed
- Validation of PAD records takes place to ensure integrity at the SEOCS receiving service
- Further validation of POca data is performed by both PEGA CRM and AVS, the latter applying business rules to accept or reject an account application
- System documentation is current, stored securely, and available to those that need it as they need it. Storage is in a SharePoint site to which approved POL staff are provided access
- HP has robust processes for the granting and removal of systems access credential

POL00393731

- System access is limited by job role. I.e. staff given the appropriate privilege for their job. i.e. role based access control
- Generic access credentials are not used
- All users are given training before being given access to live services
- All accesses to the CRM systems by CSRs are subject to audit trail. I.e. who logged on to what, when, for how long. Additionally a record of what was done during the session is made
- All access to systems by systems administrators are subject to audit trail. I.e. who logged on to what, when, for how long. Additionally a record of which commands were committed during the session is made
- HP has introduced a new online awareness campaign to educate against the perils of phishing attacks
- Cameras and camera phones are prohibited in areas where documents are received, processed, viewed and stored. They are also forbidden within the data hall areas of the data centres
- Communications between all POca partners where information being communicated is of a confidential nature are protected by encryption
- Responses to requests for customer information from authorised bodies such as the police in pursuant of a criminal investigation or prosecution are sent only in adobe acrobat pdf form to prevent manipulation. Responses are also zipped and encrypted

14.2 SEOCS

[SHAPE * MERGEFORMAT]

14.2.1 Functional Overview

SEOCS provides the capability to send and receive files to/from the Government Departments in the form of email messages, each with a single attachment containing an encrypted file having digitally signed XML representing Post Office Authorisation Documents (PAD). In essence SEOCS is a secure file transfer service.

14.2.2 Physical Environment

SEOCS is replicated across dual secure data centres in both Doxford and Washington Tyne and Wear to ensure that resilient access to SEOCS is always available in the event of loss of a single server or site.

14.2.3 Fallback processes

Should DWP not be able to provide or receive electronic PAD information via SEOCS for over 48 hours, due to the ability to transmit be lost, a manual fallback method can be invoked. This involves the Department supplying Post Office with a double encrypted disc containing the PAD information which

POL00393731

will be sent by secure courier. This data is then input using the same method as if received by secure email.

If HMRC lose their transmission capability for over 48 hours, it is documented that will print PAD records and use a secure courier service to deliver to HP. However, this process has never been used, nor has it ever been tested, and during an outage in 2012 it became evident that HMRC may not be capable of performing this agreed process as documented and contracted. This is detailed as a risk in this document.

14.3 CRM (Customer Relationship Management) system

[SHAPE * MERGEFORMAT]

The Customer Relationship Management (CRM) system was developed using a web-based CRM package called Pega Systems and is used in the POca Contact Centre. Agents log into the system, and are constrained to follow specific processes by the configured screen flow. The CRM System's main functions are to record contact history; provide a user friendly front end to the Banking System; and provide a simple method to administer workflow.

The CRM system interfaces with the following systems:

- EBT – A banking system which hosts and administers the PO Card Accounts.
- AVS – An application verification component which applies business validation rules to process POca application forms and issue account numbers.
- SEOCS – Secure, encrypted communications capability for the exchange of data needed for account opening between Government departments and POca.
- Tower Image Warehouse – A scanned document repository, holding images of all inbound and outbound correspondence.
- Fulfilment –HP Washington fulfilment centre, for the production and dispatch of outbound correspondence.
- PAF – Postal Address File. Data file of all postal addresses in UK and Ireland.
- FAD – Details of all Post Offices in the UK and their respective FAD codes.
- Phone Switch (ACD) – Distributes voice calls in the contact centre. Contains call statistics.
- MI – Management Information. Reporting information stored in Tower.
- Contact Centre – CSR terminal to POca CRM front-end
- Cheque Printing Solution – A JP Morgan application for generating cheques.

POL00393731

14.3.1 Application processing

CRM includes a java component named AVS which is used to process application data. AVS allocates POca account details to each application prior to populating application data in to the CRM tables. AVS also validates the application data against decisioning rules and approves/rejects or allows for the application to be data repaired.

14.3.2 Authentication

CRM supports the authentication of all customer calls and correspondence. EVP data is used by CRM and the CSR to enable telephone caller authentication. For back office work, CRM supports the retrieval of the image of the current recorded customer signature for comparison with incoming correspondence. Authentication of postmasters calling in via the NBSC to the POca Contact Centre is the responsibility of NBSC.

14.3.3 Contact History

CRM holds a log of all interactions and key events for each customer and provides audit information on the date, time and agent who completed the action. The contact history commences upon processing of the POca application from DMS and successful transmission of interface data between the systems, regardless of whether the application is valid at that time.

14.3.4 Inbound Correspondence

Paper items to be processed are loaded into the system via an interface to the scanning system. They are created as either non-specific paper cases (where the type of case is unknown), or specific paper cases (where the type of case is known as the paper item is a specific form). Image references are stored in each paper case. The images are viewed in a separate window, one page at a time. Mechanisms are available to allow paging, zooming and scrolling of images.

14.3.5 Outbound Correspondence

CRM supports the generation of letters and pre-populated returnable documents. For example, if a customer has failed EVP a pre-populated EVP reset form is generated at the fulfilment Centre. Bespoke letters may be required in response to a very limited number of cases e.g. court action or unusual probate cases. These are produced by authorised personnel only and printed locally. A copy is stored in Tower and linked back to the contact history of the account in CRM.

14.3.6 Message Broker

The banking system (EBT) interface is handled using fixed format message blocks. The message broker converts CRM messages into the correct EBT format, thus allowing Banking System transactions to be executed using data supplied through the scripted CRM processes.

POL00393731

14.3.7 Batch Feeds

The transfer of batch data is carried out using Connect: Direct which is a tool used to copy files from one location to another and then run any necessary scripting logic. The batch files contain data such as new applications from DMS, account updates and event history from the Banking System.

POL00393731

14.4 Tower Image repository

The Tower solution is based on centralised image storage using a Network Addressed Storage (NAS) device. The scanning solution used is the Input Accel Tower Integrated Document Management (IDM) system.

A UNIX server provides access to the storage tier and facilitates archival and retrieval of documents. The live and DR Tower systems are delivered from the secure data centres along with other POca systems

For the document repository and retrieval system:

- Tower Systems software: Oracle database server running on 2 x UNIX servers. The Tower server is used to upload document images from Swansea Input Capture, Washington Fulfilment, CRM and all the other systems for Management Information. It also distributes the electronic data captured by CMS to AVS

- CSRs retrieve image data from Tower via an interface with the front-end PEGA CRM system

- NAS storage: A NAS device provides the long-term storage of documents. The NAS device stores all documentation scanned and signatures extracted from relevant forms throughout the life of the programme.

- Batch Scheduling: the batches of images and data from Input Capture to Tower are sent throughout the day whenever the batch has completed processing. Fulfilment data is sent to Tower as part of a batch after the documents have been sent to the print queues. Data sent to AVS is sent as part of the end of day batch

- Access to any Management Information held on the Tower system for POL users is made available via the Doxford firewall. Network Address Translation (NAT) is used to redirect the traffic to the Tower system. This gives additional security for external users.

15 HP Data Centres (Doxford and Wynyard)

The data centre element of the end-to-end Information Security Risk review was postponed to ensure that the centralisation of all servers and databases was complete, and the following scope was agreed between HP and the consultant.

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

15.1 Data Centre review scope

The following was sent to HP in advance of the onsite visit:

HP Data Centre Review checklist

It is envisaged that the Information Security Risk Review of both Data Centres will be from outside in and look at both physical and environmental (fire, flood) security measures and ensuring that the required n+1 resilience is present at all levels down to server and storage component level. I.e. perimeter security, external personnel and vehicle security, CCTV, staff and visitor entry and exit procedures, site log, power, environment, networks, through to the POca specific Data Hall, and associated servers, storage units, switches, routers and backup devices.

Scope for both Doxford and Wynyard Data Centres

- Investigation of input/output routes to/from Data Centre, specifically the POca VPN
- Cable and Wireless MPLS (Multi-Protocol Label Switching) "Cloud" resilience
- Identification of any and all components that might be a single-point-of-failure (SPOF)
- Look at all areas where data is received, processed, stored, and transmitted, for POca CRM servers which deliver SEOCS, AVS, Tower, PEGA, network infrastructure, SAN (Storage Area Network) and backup devices
- Understand resilience of POca VOIP system which is routed through the Doxford Data Centre with backup through Russelsheim in Germany
- Look at all areas where data is received, processed, stored, and transmitted, for EBT and associated storage and backup devices
- Understanding of published numbers in terms of component mean-time-between-faults (MTBF)
- Power supplies: including, but not limited to, sub-station, mains supply, uninterrupted power supply (UPS)/battery backup, standby generation, server power modules, network switches and router power supply units, SAN power supply units, etc.
- Environmental units designed to monitor and regulate temperature, humidity and air cleanliness
- Equipment maintenance contract service levels with specific emphasis on controls to minimise any data loss or compromise following replacement of any data storage unit or failed/end of life backup tapes
- Links to enable mirroring to between Doxford and Wynyard and identification of any component resilience issues or SPOF
- Remote monitoring of data centres – where from? How? What can be accessed?
- High-privilege engineer credentials
- Third-party remote diagnostic links

POL00393731

15.2 Data Centre protective controls

The following control list is indicative of the very high-profile services delivered from both data centres for which customers expect high levels of protection and resilience. The list is therefore not exhaustive:

Tiered levels of availability at data centres

Tier Level	Requirements
1	• Single non-redundant distribution path serving the IT equipment • Non-redundant capacity components • Basic site infrastructure with expected availability of 99.671%
2	• Meets or exceeds all Tier 1 requirements • Redundant site infrastructure capacity components with expected availability of 99.741%
3	• Meets or exceeds all Tier 1 and Tier 2 requirements • Multiple independent distribution paths serving the IT equipment • All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture • Concurrently maintainable site infrastructure with expected availability of 99.982%
4	• Meets or exceeds all Tier 1, Tier 2 and Tier 3 requirements • All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems • Fault-tolerant site infrastructure with electrical power storage and distribution facilities with expected availability of 99.995%

15.2.1 Doxford (location for POca live systems)

- The site is anonymous and unsigned
- Dedicated dark fibre links with Wynyard
- Designed as a Tier 3 Data Centre (see table above)
- Meets government requirements. Not yet List X, but very little improvement would be needed to bring it to that status
- All data centre staff, including non-HP, site security (G4S) and building facilities (ISS) cleared to UK Government SC level
- 3 metre anti-ram/climb perimeter fence protected by razor wire, CCTV and sonic tape to provide warning of intruders
- Vehicle access by swipe/PIN card for staff. Visitors only by prior agreement and communication with building facilities before access granted

POL00393731

- Visitors only by agreement and full ID checks performed before entry
- Engineer call-outs subject to a permit-to-work (PTW) process which includes levels of access required
- Fast-track PTW process requires same levels of approval
- Internal CCTV covering all strategic points
- Swipe/PIN cards for each and every zoned access point with access limited by job function
- Network traffic routed by two diverse links with multiple carriers
- Onsite sub-station receives two 11kv power supplies from the National Grid via diverse routes. Note; single sub-station building but two rooms protected by firewall designed to last for two hours. Each room takes one of the diverse supplies and can power the whole site if required
- Two parallel UPS systems per hall offering n+1 redundancy – able to handle full load but standby generators up to full capacity within seconds
- Each UPS battery is remotely monitored
- Three standby generators support each Data Hall with n+1 redundancy; each serviceable under full load so no outage for maintenance
- Data Centre deemed part of UK Critical National Infrastructure so supplies of diesel protected and prioritised
- Power Distribution Units (PDU) fed by dual diverse supply
- Air-conditioning systems offering n+2 redundancy with all pipework in deep trenches for protection against water leaks
- Building Management System monitored 24x7x365 by onsite ISS Facilities staff
- Security/intruder system monitored 24x7x365 by onsite G4S Security staff
- Water (sprinkler) fire suppression. Note that system is not charged until alarm so dry in data halls ensuring no drips. System completely zoned so water dropped only on offending equipment. Fire suppressant gas not an option for a room of the sizes of the data halls.
- Data hall network cabling in trays above server racks as far as possible for easy access and less risk of attack from moisture or vermin
- Data Hall protected by swipe/PIN entry
- All servers, storage units, routers and switches are fully resilient offering fail-over as needed
- Remote monitoring of servers and storage from Zaragoza in Spain, with switches and firewalls from Bratislava in Slovakia. Neither of these locations have any access to data

15.2.2 Wynyard (location for POca DR systems)

- Award winning design minimises energy consumption and carbon footprint
- Designed as a Tier 3 Data Centre (see table above)
- Dedicated dark fibre links with Doxford

POL00393731

- Meets government requirements. Not yet List X, but very little improvement would be needed to bring it to that status
- All data centre staff, including non-HP, site security (G4S) and building facilities (ISS) cleared to UK Government SC level
- 3 metre anti-climb perimeter fence protected by razor wire, CCTV and sonic tape to provide warning of intruders
- Car park separated from data centre by similar fencing
- Vehicle access by swipe/PIN card for staff. Visitors only by prior agreement and communication with building facilities before access granted
- Truck access via separate "air-locked" entrance. i.e. anti-tailgating configuration
- Visitors only by agreement and full ID checks performed before entry
- Engineer call-outs subject to a permit-to-work (PTW) process which includes levels of access required
- Fast-track PTW process requires same levels of approval
- Electronic beam, motion detection and CCTV throughout
- Swipe/PIN/fingerprint entry depending on sensitivity of zone
- Access to data halls via anti-tailgating pods with fingerprint required for entry
- Access to all server/storage cabinets limited to those named on PTW
- Keys for server cabinets on electronically secure board; only available to engineer with appropriate PTW. Cannot exit data hall without return of key into appropriate slot
- Network traffic routed by two diverse links
- Power is supplied from the National Grid via 2 x 66kv supplies in redundant configuration.
- Each data hall is supported by 3 x UPS systems per hall offering n+1 redundancy – able to handle full load for 15 minutes but standby generators up to full capacity within seconds
- Each UPS battery is remotely monitored
- Standby generators support each Data Hall with n+2 redundancy; each serviceable under full load so no outage for maintenance
- Data Centre deemed part of UK Critical National Infrastructure so supplies of diesel protected and prioritised
- Power Distribution Units (PDU) fed by dual diverse supply
- Standard air-conditioning systems are not used. Instead, air is brought into the building by 8 x 2.1m diameter axial fans offering n+2 redundancy. Air is filtered and humidified as required automatically and cools equipment racks from under the data hall floor. Warm exhaust air is extracted by another 8 x fans of the same size. A portion of the exhaust air is mixed with incoming air to manage appropriate environmental conditions
- Building Management System monitored 24x7x365 by onsite ISS Facilities staff
- Security/intruder system monitored 24x7x365 by onsite G4S Security staff

POL00393731

- Water (sprinkler) fire suppression. Note that system is not charged until alarm so dry in data halls ensuring no drips. System completely zoned so water dropped only on offending equipment. Fire suppressant gas not an option for a room of the sizes of the data halls.
- Data hall network cabling in trays above server racks as far as possible for easy access and less risk of attack from moisture or vermin
- All servers, storage units, routers and switches are fully resilient offering fail-over as needed
- Remote monitoring of servers and storage is performed from Zaragoza in Spain, with switches and firewalls monitored from Bratislava in Slovakia. Neither of these locations have any access to data

16 Main areas of risk (Government)

16.1 PAD record transmission and deletion

Risk: (HIGH) Availability

Operational; Criminal; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Post Office has strict controls around the use, processing, storage and secure destruction of paper records which include customer personal information. It is not known whether or what controls exist at initiating Government offices, e.g. Job Centre Plus in terms or records of POca applicants. Insecure or poor controls risks compromise which could impact detrimentally not only Government departments, but also Post Office.
2. Some POca customers have difficulties using PIN Pads, and more customers are struggling to pass EVP authentication on the phone. This presents a challenge to Post office staff. On the one hand they are told to be helpful to customers, on the other, assisting with PIN entry and/or keeping cards behind the counter for customers puts the customer in breach of the product terms and conditions, and also opens staff up to accusations of fraud and theft, which would be difficult to deny. We need to be mindful that UK citizens are living longer but frailty, infirmity, and loss of faculties are affecting some of them, leading to difficulties in seemingly simple tasks
3. Although it has not been possible to conduct a review of the Government departments' PAD production processes and sending infrastructure, we do know that the planned power outage at the Norcross Data Centre over Easter 2011 caused the loss SEOCS transmission capability, which identified that the Enterprise Business Gateway (EBG) at Norcross does not have a failover partner. This increases the risk that POca will have to invoke the SEOCS

POL00393731

fallback in that a "force-majeure" in that domain would put us into a Fallback scenario.

4. The Easter 2011 SEOCS incident highlighted also that files were being deleted purely on the passage of time. Moreover, the time period had been reduced from 5 days to 2 days unbeknown to EBG Support or MoPR (DWP Method of Payments). File deletion purely on the passage of time, regardless of processing success criteria , whether 2 days or 5 days goes against best practice
5. The HMRC incident (August 2012) where loss of the PGP Desktop encryption software on their desktop PC caused the failure to transmit tax credit customer PAD records for seven working days. This highlighted the fact that the sending PC is a single-point-of-failure. A second PC was thought to be available but the setup was not to the required build. Until resolved, there is an ongoing high risk that HMRC will fail to transmit the required PAD files thereby impacting citizens requiring tax credit payments and/or child benefit. This event could lead to adverse PR for POL in that customers will likely assume POca to be at fault. This will also increase the likelihood of invoking the fallback process, which has never been used, and when discussed with HMRC may not have worked if invoked

Recommendations

16.1.1 It is recommended that a review of record handling and secure destruction processes is performed at initiating Government offices to minimise compromise or loss; unless such a review has been performed and the results were satisfactory

16.1.2 All must be aware of the risk that single-points-of-failure in critical processes pose. We should take comfort that we now have a workable SEOCS fallback arrangement for DWP (copy PAD records to double encrypted disc) as opposed to the paper based arrangement which would have been costly in resource, and probably not doable in reality

16.1.3 The PAD file deletion process should be enhanced to at least five days (although the actual value would be identified as part of an impact assessment), but with the addition of file processing success criteria: i.e. "IF > 5 days AND success message received THEN delete file"

16.1.4 HMRC should urgently review their reliance on desktop PC(s) for PAD file delivery, the second of which must match the build of the primary and be fully documented as such in operational procedures. Each should also have enhanced support over and above the standard desktop fix when broke service provided by Aspire (delivered by Cap Gemini). The two desktops should of course also be in two separate building for resilience purposes

16.1.5 It is recommended (and has been agreed with DWP and HMRC) that a full walk-through, of the HMRC (paper) Fallback arrangement should be performed to ensure that if invoked, the process will work. It is

POL00393731

recommended that a rehearsal be agreed to ensure the process will work in reality

16.1.6 If the walkthrough and rehearsal prove problematic, serious consideration should be given to replicating the agreed DWP fallback procedure of copying PAD records to double encrypted disc with secure hand-delivery

16.2 Vulnerability to phishing and spear-phishing attacks

Phishing emails are designed to fool users into clicking on a malicious link which could be designed to harvest personal and corporate logon credentials, bank details or other financial or personal information; this is the more modern form of Social Engineering attack. A more targeted act, referred to as Spear-Phishing is to focus on specific individuals within a company following an element of research, and to tailor the emails accordingly in order to dupe the recipient into visiting fake websites or activate malicious links which would unwittingly activate a malicious payload.

This kind of attack is very much on the increase with many companies behind the curve in terms of education and awareness campaigns. See the following Computer Weekly articles for more detail

[HYPERLINK "http://www.computerweekly.com/opinion/Dont-Get-Spiked-by-a-Spear-Phisher"]
[HYPERLINK "http://www.computerweekly.com/news/2240176040/UK-office-workers-swamped-with-phishing-emails-study-finds?utm_medium=EM&asrc=EM_EDA_20309056&utm_campaign=20130115_UK%20office%20workers%20swamped%20with%20phishing%20emails,%20study%20finds_&utm_source=EDA"]

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. **[HYPERLINK "http://en.wikipedia.org/wiki/Phishing%20"]** and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**, which led the firm to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to

POL00393731

highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain, but for all intents and purposes, the "mark" is sent an email, possibly from a seemingly reliable source (which has been previously compromised), with a malicious payload designed to harvest logon credentials and/or other corporate confidential information, which could lead to compromise of customer databases

Recommendations

16.2.1 ***Each firm and government department should consider its vulnerability to this kind of attack, the impact of loss and/or compromise, and the awareness of staff to the dangers. They must consider what steps can be taken to minimise the threat as part of their Information Security Awareness programmes. A good start will be to visit [HYPERLINK "http://www.antiphishing.org"] and download the report entitled "Phishing Activity Trends Report 1st Quarter 2012". Note that the headline states "Financial Services continued to be the most targeted industry sector in the first quarter of 2012. [p. 7].*** **It is also recommended that firms consider as part of their campaigns the deliberate and controlled targeting of key members of their own staff (and executives) in mock exercises by means of available tools, such as [HYPERLINK "http://www.phishme.com"]. This is an example not an endorsement of the company delivering this service**

17 Main areas of risk (Post Office Counters)

17.1 POca cash withdrawal transactions

Risk: (HIGH) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability, business and agent debt); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The "withdraw limit" transaction, which enables the removal of all funds in the POca displays only the words "withdraw limit" to the customer on the PIN Entry Device (PED) – pre-Ingenico. This creates the risk that the customer will have a legitimate reason for dispute, and that the FSA/FoS might side with the customer, in that the customer is not authorising a specific value. The fact that the actual transaction amount is not displayed to the customer is also an enabler for Counter clerk fraud.
2. The "withdraw limit" transaction is significantly overused in all outlets at nearly 70% of the total cash withdrawals, and has in fact become the norm, with Counter Clerks asking the customer, "*Do you want all of it today*"? Its overuse leads to transaction disputes in that the value is not displayed on the

POL00393731

PED, and in some cases the customer receives more money than they expect, e.g. when winter fuel allowances have been added, or the week before a Bank Holiday when pensions are doubled. Its general use is also in contravention of the Counter Operational manual, which states, *"Ask the customer how much cash they wish to withdraw"*

3. Malicious withdrawal from a POca is possible by a criminally minded Counter Clerk. E.g. deliberately misinforming the customer that the transaction has failed, and that the PIN should be re-entered has happened, as has the misuse of "withdraw limit". E.g. customer asks for £300, but "withdraw limit" used leading to theft of funds above £300, up to the £600 day limit. Customers may only become aware of the theft if and when they check their quarterly statements.
4. Where fraud is committed the transaction receipt is not usually provided to the customer, or the receipt of someone else's transaction is given instead in the hope that it will not be scrutinised. This is enabled by the fact that customers are not educated to ask for one.
5. Some POca customers have difficulties using PIN Pads. This presents a challenge to Post office staff. On the one hand they are told to be helpful to customers, on the other, assisting with PIN entry and/or keeping cards behind the counter for customers puts the customer in breach of the product terms and conditions, and also opens staff up to accusations of fraud and theft, which would be difficult to deny. We need to be mindful that UK citizens are living longer and longer but frailty, infirmity, and loss of faculties are affecting some of them, leading to difficulties in seemingly simple tasks. Note that this issue has been recognised by other banks and the UK Payments Council commissioned report is linked here:

[HYPERLINK "http://www.paymentscouncil.org.uk/files/payments_council/payments_council_-_policis_and_toynbee_hall_older_old_and_disability_report_24.10.12_final.pdf"]

6. The POca product does not offer chip/signature as an option for customers who cannot operate a PIN pad. It is though highly likely that anyone who has such issues would be unable to present a signature that could be validated, or indeed fit a signature on the strip of the card. The lack of options though could risk adverse publicity for Post Office for not offering disabled customers the option. Note that the Which Consumer organisation has published a mystery shopper report on the subject

[HYPERLINK "http://www.which.co.uk/news/2012/01/banks-are-declining-chip-and-signature-requests-276944/"]

7. As customers age they are also struggling to authenticate themselves over the phone at the POca Contact Centre in that their ability to recall their memorable

POL00393731

information is decreasing, and in many instances cannot even understand the questions put to them. If customers are denied access to their accounts it is not only a risk to the public image of POL, its partners and DWP, it could lead to denial of "food on the table" benefits

8. It is possible to mis-key withdrawal values in Horizon in that the value is entered and once the ENTER key is depressed the transaction is committed. This issue also impacts partner banks in that both withdrawals and deposits are impacted by the lack of transaction integrity checks at point of entry.

Recommendations

17.1.1 Counter staff must be discouraged from asking customers "do you want it all?" They must be encouraged to follow the existing instruction in the Counters Operational Manual: i.e.

For Cash Withdrawals

- Select Withdrawal
- Ask the customer how much cash they wish to withdraw
- Input the required value then press Enter

For Withdrawl limit

- Select Withdraw Limit

17.1.2 The value of the withdraw limit transaction should be displayed on the PIN Entry Device.

NOTE: This control recommendation has been made in previous reports and will be introduced during the PIN Pad replacement project, which will replace all (some 30,000) PIN Pads (with Ingenico iPP3550 devices) across the POL estate. The following is copied from the project presentation.

"POCA Withdraw All – Change to process. The value of the withdrawal will be displayed on the Pin Pad screen and customer must confirm before the clerk can proceed with the transaction"

POL00393731

17.1.3 All Post Office staff, particularly at times when additional payments are likely to have been deposited (winter fuel/double pension), should be told to ensure, that before withdrawal they are to inform the customer that there may be more money in the account than usual, and that it might be best to withdraw a specific value or do a balance check in advance.

17.1.4 Requiring the customer to enter the value of the withdrawal as they would at an ATM is also an option. This option would negate the need for the counter clerk to enter the value. It is recommended that the clerk checks and agrees the value before commitment and PIN entry to minimise error. We should though bear in mind that some customers struggle with PIN entry so inputting the value also might be an issue

17.1.5 Serious consideration should be given to the publicity around the whole of Post Office that staff have been tempted to steal from customers, particularly the old and vulnerable. These people have received prison sentences. Publicising these cases should act as a deterrent to those inclined to take advantage of weaknesses is processes and systems

17.1.6 A small, but neat and bold (no more than A5 size, and possibly A6) prominent notice should be placed at every counter position stating "please ensure you obtain and keep your receipt. It will be needed should you wish to contact us about your transaction"

17.1.7 When a customer struggles to use the PIN Pad, they should be politely steered to the Permanent Agent process.

17.1.8 Where a customer cannot operate a POca, and they do not have a trusted carer, friend or relative to operate the account on their behalf, Post Office should be asking whether POca is the best method for their benefit payments. Discussions should be considered with DWP in that UK citizens are living longer, yet their ability to operate financial products is often diminishing. Is POca right for all? Are there alternatives that are safer and less demanding?

17.1.9 New Ingenico PIN Pads are being rolled out in every outlet. These devices have "contactless" capability. Post Office should investigate this functionality in that it may be a way that we could help our aging and infirm customers remain customers. I.e. provide a contactless card which must be accompanied by a face-to-face identity check

17.1.10 Serious consideration should be made in conjunction with DWP and UK government, of a possible biometric identity scheme that would prove a citizens' identity even if they cannot adequately enter a PIN or remember verification detail. This could be an opportunity for the Post Office in that we have the Application, Enrolment and Identity (AEI) booth

17.1.11 Post Office senior managers and Executives visit the front-line Post Offices at regular intervals. The POca Contact Centre is very much "front line" in terms of customer contact. It is recommended that some POL executives spend a day in the Contact Centre listening to customer calls to understand the difficulties detailed above

POL00393731

17.2 P6167 – Account Closure process

Risk: (HIGH) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability, business and agent debt); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. P6167 POca Account Closure form requires only the customer's name and address, a valid signature and the 16-digit PAN of the POca for an account to be closed and either a cheque or credit transfer to be initiated. This can (and has) provide someone with criminal intent who is close to the PAH, a rogue Contact Centre Customer Service Representative, or Counter Clerk with an opportunity to close an account and divert funds.
2. HP PEGA CRM system is used to manage all customers' servicing. It should be noted that one EDS (precursor to HP) CSR was sent to prison for six months for taking advantage of the weak account closure process by information gleaned from the "gone away" procedures. I.e. scanned envelopes indicates "returned to sender"; balance is in credit and substantial; no deposit or withdrawal history for xx months but still not dormant. This indicates the customer is likely to be dead without an estate or anyone to stake a claim; all information available to make a malicious closure and funds transfer

Recommendations

17.2.1 Post Office – introduce a face-to-face identity check at the counter to ensure that the PAH is presenting the P6167. Also make it mandatory that the PAH is the payee for either cheque or credit transfer

17.2.2 Post Office – consider a prompt to the counter clerk ("have you changed address? Please call the POca Contact Centre") when a customer presents with a POca for withdrawal if HP has reported that correspondence has been returned to sender. This would require a message to be passed via EBT to Horizon

17.2.3 HP – For the "gone away" process only, remove the balance and account details from the left side of the PEGA screen. Presenting the account details adds no value but provides opportunity for accounts with credit balances and no withdrawal history for xx months

17.2.4 JP Morgan – consider the following

IF POca balance > £xxx

AND no deposit or withdrawal transactions for xx months

THEN Freeze account

POL00393731

17.3 Banking (and other free-form value entry transactions) mis-keys

Banking transactions are suffering from a large mis-keying problem, which leads to customer frustration, business losses, agent debt, and increased level of fraud, productivity issues, and the business embarrassment of asking partner banks for reversals. Banking transactions interface with the Link Network in real time. I.e. once committed the funds become cleared and available at a Post Office, Bank counter or ATM, regardless of whether mis-keying has taken place.

The mis-keying issue though affects a broad range of products including DVLA, Bill Payments, Personal Banking, Post Office Card Account and Business Banking.

Risk: (HIGH) Integrity, Availability, Fraud

Impact: Financial (product profitability, business and agent debt); marketability of future financial, banking and bill payment products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; Banking/Bill Payment partner confidence.

1. Non-validated, free form entry of transaction value can cause accidental and possible deliberate mis-keying, which leads to source data integrity issues, and a high volume and value of compensating transactions in relation to banking. Note that once committed, the transactions become cleared funds via the Link Network, and in some situations over deposits have been withdrawn. This leads to business losses, agent debt, management and productivity issues, and is detrimental to partner/client relations.

Recommendations

17.3.1 Serious consideration should be given to the double entry of the requested value of both withdrawal and deposit transactions. Cross-validation of the two entries will dramatically reduce the mis-keying problem, which is being experienced on banking and other transaction.

NOTE: There is a project looking at this issue within Post Office – Key contact:

Karen Hillsden – Principal Analyst
Postline: GRO
Mobex: GRO

There will of course be a one-off cost for the change, testing, and counter communications, but it should be borne in mind that the benefits and savings will be ongoing and recurring.

POL00393731

IMPORTANT NOTE: The roll-out of new Ingenico PIN pads will also see the following recommendations from the Consultant's previous report (dated 15th July 2008) actioned: i.e.

- **Banking Deposits – Change to process. The value of the deposit will be displayed on the Pin Pad screen and customer must confirm before the clerk can proceed with the transaction**

- **POCA Withdraw All – Change to process. The value of the withdrawal will be displayed on the Pin Pad screen and customer must confirm before the clerk can proceed with the transaction**

17.4 POL receipt, storage and deletion of POca customer personal documentation and voice recordings

Risk: (MEDIUM) Confidentiality

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image

1. Some Post Office personnel, (notably but not necessarily exhaustive) Security, Information Security, Network and Managed Services receive customer details to aid decisions on transaction disputes, claims and investigations. JP Morgan also sends details from their fraud filters which contain sensitive information subject to the protection of DPA 1998. This data should be sent and received in encrypted form, and whilst resident on laptops is encrypted. However, saving of attachments to networked drives, in particular shared team drives means that the data is stored in clear text on those servers. Microsoft Outlook emails and attachments are stored in Cloud services but these are resident within the EEA, so conforms to the requirements of DPA1998
2. Sample voice recording are to be supplied the POca product team. Controls have been agreed to ensure that discs containing these recordings are fully encrypted. There is though a risk that voice data might be copied to laptops, and/or leave temporary files behind after listening. It should be noted that these recordings will include customers' EVP questions and answers so protection is vital

Recommendations

POL00393731

17.4.1 Agreement should be reached with the POL Head of Information Security as to advice, guidance and instructions in relation to the receipt, storage and deletion of customer personal data. Although this risk is in relation to POca data, the same risk will no doubt apply to other areas of the Post Office business, so any control should be generic and communicated across the whole business

17.4.2 Information Security controls will be agreed and documented to ensure that discs containing voice recordings and any electronic copies are protected during receipt, travelling, use, retention and secure deletion, which will include customers' EVP questions and answers

17.5 Post Office POca documentation

Risk: (Low) Integrity, Availability

Impact: Operational.

1. Some documents produced at project stage have not been reviewed and updated, particularly TIS documents owned by POL. This presents a risk that documents will be read as current when they are not

Recommendations

17.5.1 HP and POL need to agree which documents require review and to agree a timetable for regular review and update

17.6 Vulnerability to phishing and spear-phishing attacks

Phishing emails are designed to fool users into clicking on a malicious link which could be designed to harvest personal and corporate logon credentials, bank details or other financial or personal information; this is the more modern form of Social Engineering attack. A more targeted act, referred to as Spear-Phishing is to focus on specific individuals within a company following an element of research, and to tailor the emails accordingly in order to dupe the recipient into visiting fake websites or activate malicious links which would unwittingly activate a malicious payload.

This kind of attack is very much on the increase with many companies behind the curve in terms of education and awareness campaigns. See the following Computer Weekly articles for more detail

[HYPERLINK "http://www.computerweekly.com/opinion/Dont-Get-Spiked-by-a-Spear-Phisher"]
[HYPERLINK "http://www.computerweekly.com/news/2240176040/UK-office-workers-swamped-with-phishing-emails-study-finds?utm_medium=EM&asrc=EM_EDA_20309056&utm_campaign=20130115

POL00393731

UK%20office%20workers%20swamped%20with%20phishing%20emails,%20study%20finds&utm_source=EDA"]

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. [HYPERLINK "http://en.wikipedia.org/wiki/Phishing%20"] and [HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"] attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including [HYPERLINK "http://www.emc.com/security/index.htm"], which led the firm to [HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"]. This attack was followed by a [HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"] which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain, but for all intents and purposes, the "mark" is sent an email, possibly from a seemingly reliable source (which has been previously compromised), with a malicious payload designed to harvest logon credentials and/or other corporate confidential information, which could lead to compromise of customer databases

Recommendations

17.6.1 ***Each firm and government department should consider its vulnerability to this kind of attack, the impact of loss and/or compromise, and the awareness of staff to the dangers. They must consider what steps can be taken to minimise the threat as part of their Information Security Awareness programmes. A good start will be to visit [HYPERLINK "http://www.antiphishing.org"] and download the report entitled "Phishing Activity Trends Report 1st Quarter 2012". Note that the headline states "Financial Services continued to be the most targeted industry sector in the first quarter of 2012. [p. 7].*** **It is also recommended that firms consider as part of their campaigns the deliberate and controlled targeting of key members of their own staff (and executives) in mock exercises by means of available tools, such as [HYPERLINK "http://www.phishme.com"]. This is an example not an endorsement of the company delivering this service**

17.7 POca transaction drop-offs and corresponding peaks

POL00393731

Risk: (MEDIUM) Availability

Impact: Regulatory; Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image

1. HP/JPM has reported to POL that they are seeing a drop off of POca transactions as seen by the JPM EBT system. This is immediately followed by a spike of transactions up to 350 TPS. The POca service has only been tested to 240 TPS. This could impact the JPM service targets which require that they manage 95% of transactions in 2 minutes and 100% in 10 seconds. There is also a view that as the cause is not known an increase in POca transactions at peak volume times, e.g. double pension days in advance of Bank Holidays may cause transaction queuing. The risk is that customers will notice a wait as transactions take longer to commit at the PIN Pad, and in worst case scenario timeouts may occur

Recommendations

17.7.1 HP/JPM has monitored from the EBT receiving side and have stated that the problem is not there; the cable and wireless link has also been discounted as possible cause. Fujitsu delivered graphs which display transaction throughput at only 5-minute periods so this does not help. In order to progress this issue, Fujitsu will need to monitor between HNG and the sending router in order to provide the same sub-second level of granularity which HP/JPM has delivered

17.8 Horizon Terminal time offsets

Risk: (MEDIUM) Integrity; Availability

Impact: Regulatory; Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image

1. JP Morgan are reporting that out of a sample of 865,731 transactions from 10,643 FAD codes, 1,640 FAD codes had at least one terminal with "its time out by more than 1 minute (±1.0 second). And of those, 36 FAD codes had at least one terminal with its time out by more than 5 minutes, with the worst one being out by nearly 21 minutes. This indicates that clock synchronisation at the counter is not always what it should be. JP Morgan has a service level to perform transactions at 95% within 2 seconds and 100% within 10 seconds so terminal time offset can impact. The risk is that banking transactions (including POca) which generate a customer dispute may rely on the time stamp on the receipt which may need to be used for evidential purposes, but if

POL00393731

this is offset considerably to the time of the transaction recorded by the bank complications could arise

Recommendations

17.8.1 Fujitsu should investigate this issue as previously reported and respond accordingly

POL00393731

Main areas of risk (HP Input Capture Centre)

17.9 Server room fire suppression system

Risk: (MEDIUM) Availability

Impact: Operational

1. The server room door is directly opposite the Kelly Services office, and immediately to the side of the server room door is a bright red button, which the Consultant was informed is the activation button for the fire suppressant gas. It is assumed (although not confirmed) that should the button be pressed when the door is locked, fire suppressant will be released. The positioning of this button could lead to accidental release of gas, and due to the close proximity of Kelly Services, there might be a scenario when an agency staff member may be disciplined and could release the gas maliciously.

Recommendations

17.9.1 Consider the protection of the fire suppressant gas release button by means of a flap, or box of some description in order to hide its purpose, and reduce the chances of accidental or malicious operation

17.10 Confidential waste

Risk: (MEDIUM) Confidentiality, Fraud

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. All documents are stored for a period of one calendar month following scanning. They are then put into locked bins for secure disposal. Keys to these locked bins are held by the building facilities company, ISS who also manage the secure disposal contract. This creates a risk that customer personal POca documents could be accessed for nefarious means, out of office hours with little chance of discovery.

Recommendations

POL00393731

17.10.1 Remove keys from the stewardship of ISS and bring back into HP control. I.e. within the locked key cabinet in Leigh Gough's office, which should be locked out of normal working hours

17.11 Development and support skills sharing

Risk: (MEDIUM) Availability

Impact: Regulatory; Contractual: Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The main expert in relation to Input Accell – Dispatcher is John Cavell. John could be regarded as a single-point-of-failure and if he chose to leave HP or became long-term absent, there could be a detrimental effect on operational continuity

Recommendations

17.11.1 Ensure that skills and knowledge that John Cavell has in terms of Swansea Input Capture processes and technologies are replicated elsewhere to minimise risk of loss

17.12 Firewall infrastructure changes

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Regulatory; Contractual: Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The firewall infrastructure in Swansea has recently been replaced with HP proprietary equipment. Although data is held on servers from no more than five days, there are risks following major infrastructure changes that could be introduced, especially if firewall configuration changes are made

Recommendations

17.12.1 It is recommended that a Penetration Test be performed by a CESG [HYPERLINK "http://www.cesg.gov.uk/servicecatalogue/CHECK/Pages/WhatisCHECK.aspx"] approved provider to minimise malicious entry, data loss or compromise.

17.13 Vulnerability to phishing and spear-phishing attacks

POL00393731

Phishing emails are designed to fool users into clicking on a malicious link which could be designed to harvest personal and corporate logon credentials, bank details or other financial or personal information; this is the more modern form of Social Engineering attack. A more targeted act, referred to as Spear-Phishing is to focus on specific individuals within a company following an element of research, and to tailor the emails accordingly in order to dupe the recipient into visiting fake websites or activate malicious links which would unwittingly activate a malicious payload.

This kind of attack is very much on the increase with many companies behind the curve in terms of education and awareness campaigns. See the following Computer Weekly articles for more detail

[HYPERLINK "http://www.computerweekly.com/opinion/Dont-Get-Spiked-by-a-Spear-Phisher"]
[HYPERLINK "http://www.computerweekly.com/news/2240176040/UK-office-workers-swamped-with-phishing-emails-study-finds?utm_medium=EM&asrc=EM_EDA_20309056&utm_campaign=20130115_UK%20office%20workers%20swamped%20with%20phishing%20emails,%20study%20finds_&utm_source=EDA"]

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. **[HYPERLINK "http://en.wikipedia.org/wiki/Phishing%20"]** and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**, which led the firm to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain, but for all intents and purposes, the "mark" is sent an email, possibly from a seemingly reliable source (which has been previously compromised), with a malicious payload designed to harvest logon credentials and/or other corporate confidential information, which could lead to compromise of customer databases

Recommendations

POL00393731

17.13.1 ***Each firm and government department should consider its vulnerability to this kind of attack, the impact of loss and/or compromise, and the awareness of staff to the dangers. They must consider what steps can be taken to minimise the threat as part of their Information Security Awareness programmes. A good start will be to visit [HYPERLINK "http://www.antiphishing.org"] and download the report entitled "Phishing Activity Trends Report 1st Quarter 2012". Note that the headline states "Financial Services continued to be the most targeted industry sector in the first quarter of 2012. [p. 7].*** **It is also recommended that firms consider as part of their campaigns the deliberate and controlled targeting of key members of their own staff (and executives) in mock exercises by means of available tools, such as [HYPERLINK "http://www.phishme.com"]. This is an example not an endorsement of the company delivering this service**

Note: Since writing this report, HP has shown the Consultant a very good online education and awareness application to highlight the risks of phishing attacks which is used within their company but it is not known whether all staff close to POca have received the training.

POL00393731

18 Main areas of risk (HP Washington Fulfilment Centre)

18.1 Printing and stacking

The overall Technical Environment Document for Washington Fulfilment states that: *all multipage documents will be trimmed and nest folded once (a simple "zig zag" fold – not complex double folding)*

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud (ID Theft)

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. During the witnessed print run it became obvious that "simple zig-zag" folding does not always happen as easy as would be hoped, and takes quite a bit of operator intervention. The hopper on the printer in question through was said to be a little old. If, as does happen the operator cannot manage every fold, the weight of the following pages forces new folds not on the perforation, thereby creating pages with two or more folds or weak points. This increases the risk that jams will occur during the stuffing and enveloping process, which in turn increases the risk of human error during jam management, which then increases the possibility that customer statement pages may be sent to the wrong recipient, thereby creating a data protection incident

Recommendations

18.1.1 HP should consider whether improvements can be made to the printer stacking capability, including consideration of perforation quality and/or whether the printer hopper is beyond reasonable use

18.2 Envelope stuffing limitations and changes to statement frequency

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud (ID Theft)

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

POL00393731

The overall Technical Environment Document for Washington states that: *all stationery, envelopes & inserts will meet mailing manufacturer's guidelines for automatic insertion*

1. As part of an initiative to reduce cost, the POca customer statement frequency default is being changed from 3-monthly to 6-monthly with customers given the option to choose to revert to 3-monthly or opt for 1-monthly. However, it was discussed during the visit to Washington that any envelope stuffed with more than 12 inserts tends to jam. The change, which anticipates the vast majority of statements will be delivered twice per year, will increase the likelihood that more than 12 inserts will be required. This increases the risk of jams thereby increasing the need for manual intervention and the likelihood of human error, raising the chances that customer statement pages may be sent to the wrong recipient, causing a data protection incident

Recommendations

18.2.1 ***The possible 12-page limit should be kept under review and envelopes in excess of this number proven as part of testing to ensure that they do not initiate a higher proportion of paper jams***

18.3 Enveloping and stuffing jam management

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud (ID Theft)

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There were 22 jams witnessed during stuffing and enveloping of 5864 statements. This was said to be high but not necessarily out of the ordinary. All spoils and associated envelopes were put to a table top. By the end of the print run the table was quite strewn with envelopes and statements. Although all pages were stuffed into the correct envelopes the untidy nature of the process may on the face of it to increase the likelihood of human error, which in turn increases the possibility that customer statement pages may be sent to the wrong recipient, thereby creating a data protection incident

Recommendations

POL00393731

18.3.1 Consideration should be given to the placement of a plastic "in/out" type tray for each individual paper jam, and to top this with a plain piece of paper to minimise any possibility of cross contamination with spoils from later jams. This should keep each jam separate thereby minimising the possibility of error during manual stuffing

18.4 Staff records

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The HP Contact Centre Operations team have excellent staff records which follow the employee through their career and document key events. This provides a good record of career events such as promotion, maternity/paternity leave, and also the levels of privilege to a POca IT systems, and physical access rights (swipe card). This is not the case though for Swansea or Washington staff, nor POca IT systems or database administrators. Although not seen as a major risk, recording the same information for all HP staff that have access to POca systems will be of benefit

Recommendations

18.4.1 HP should consider extending best practice by reuse of the Contact Centre Operations process for POca employee tracking

19 Main areas of risk (HP Preston Contact Centre)

19.1 Criminal incident investigation (forensic readiness)

Risk: (HIGH) Confidentiality, Integrity, Availability, Fraud

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There have been frauds committed by CSRs in the past, most notably those discovered in 2006. POL and its partners tend to treat each as they arrive in isolation, moreover there has been occasion when POL Information Security were not made aware by POL Physical Security of an investigation, which meant that the gaps in processes and systems that were exploited still existed a year later. Unless and until there are procedures which automatically kick in,

POL00393731

which includes all stakeholders, there remains a risk that crimes may not be successfully prosecuted and that the modus operandi might be reused by others. Moreover, not all stakeholders are provided with any updates during the prosecution stages or outcomes of court cases

Recommendations

19.1.1 It is recommended that POL Information Security, POL Security, HP and JP Morgan together considers the creation and rehearsal of a criminal incident response plan which should also include a forensic readiness capability to ensure that evidence can be gathered and ringfenced to standards required by courts. Although a very difficult decision, this may even require the invocation of Disaster Recovery to enable forensic copies of live databases to be taken to prove who did what, when, how and for what purpose.

19.1.2 Notwithstanding the need for discretion and sensitivity it is important that relevant stakeholders are kept informed of prosecution progress and outcomes of court cases

19.2 Access to the public internet

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Following previous Information Security Reviews great improvements have been made, particularly to Contact Centre risks. Full lockdown of USB ports and the ability to audit printing is now present. Although CSRs and other staff do need access to the public internet, access to facilities such as webmail might still present an opportunity for malicious data loss or compromise through access to personal email

Recommendations

19.2.1 It is recommended that HP considers the risk and likelihood that a rogue CSR could or might copy and remove from site data electronically via webmail, web based Internet Messaging, or other means without detection. Although not considered to be very likely we must bear in mind that CSR fraud and targeting of POca customer accounts has happened, some of which have successful prosecution of offenders

19.3 Telephony outages

Risk: (LOW) Availability

POL00393731

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There have been a number of incidents in the past year which have impacted telephony capability at both Warrington and Preston. Although the majority of these incidents have been transparent to the end customer, they seem to be happening quite regularly

Recommendations

19.3.1 It is understood that these incident may be due to the reconfiguration of old EDS networks into HP networks since the company was taken over. Post Office would like to understand if this situation is likely to continue and if so for how long

19.4 Telephony outages (DR call plans)

Risk: (LOW) Availability

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There is a good process for coping with POca telephony failures. Depending on the scenario one of five Call Plans (B, C, D, E or F) will be invoked. However, in August 2011 a fault required the invocation of Call Plan F out of hours which wasn't fully understood. There is a risk that out of hours lost-stolen service may be unavailable if Call Plan F is not invoked to plan.

Recommendations

19.4.1 It is recommended that a rehearsal of Call Plan F be scheduled to ensure that the process is understood out of hours by both POL Duty Manager and BT

19.5 Handoff from Tier 1 CSR to Tier 2 CSR

Risk: (LOW) Availability, Customer Experience

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Handoff from Tier1 to Tier 2 CSRs is not automatic so when handoff is needed the Tier 1 CSR attempts transfer but often gets the response "I'm not available as Tier 2" (or words to that effect). This risks the possibility that the customer may drop off the call if transfer is not slick

POL00393731

Recommendations

19.5.1 It is recommended that HP look at possible ways of improving the handoff from Tier 1 to Tier 2

Risk: (LOW) Availability

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

19.6 Customer Statement requests

Risk: (LOW) Availability

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Requests from customers for copies of printed statements are handed off to Tier 2 from Tier 1. Although not strictly speaking a risk, this seems on the face of it an unnecessary process for little gain

Recommendations

19.6.1 Review the rationale that statement requests can only be performed by Tier 2, and if no obvious security or operational reason allow Tier 1 to make the requests

19.7 Sensitive transaction and levels of EVP

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Some transactions (PIN Unblock, LCW, and PBR) are denied if customers cannot pass EVP at levels 1 or 2. This is due to the fact that EVP level 3 relies only on what could be deemed as "publicly available data". Also, Tier 2 and above are required to perform the necessary authorising transaction. The consultant observed handover and Tier2 questioned "have you taken the customer through EVP"? There is a risk that Tier 2 may authorise a sensitive transaction when the customer passed EVP at level 3. It might be possible for

POL00393731

an imposter to pass at Level 3, which is why we have limited these transactions

2. The use of EVP level 3, which makes use of "publicly available data", is deemed to be "bad practice" by the FSA as detailed in their report published in 2008 entitled **[HYPERLINK "http://www.fsa.gov.uk/pubs/other/data_security.pdf"]**. It is true that this presents a level of risk that an account might be taken over by a criminal, but due to the demographic of the POca customer base, and the UK's ever aging citizenry, removal of this facility could impact the availability of "food-on-the-table" benefits, and cause alarm to customers and adverse PR to the Post Office and its partners

Note that this issue has been recognised by other banks and the UK Payments Council commissioned report is linked here:

[HYPERLINK "http://www.paymentscouncil.org.uk/files/payments_council/payments_council_-_policis_and_toynbee_hall_older_old_and_disability_report_24.10.12_final.pdf"]

Recommendations

19.7.1 HP should review handover from Tier 1 to Tier 2 to ensure that Tier 2 are fully aware of the level of EVP passed

19.7.2 HP should consider where PIN Unblock, LCW or PBR are requested that the handover should be immediate and that Tier 2 perform the EVP process

19.7.3 The POca Risk Steering Group has documented the risk associated with EVP level 3 and the possibility that the FSA will pick this up in an audit as "bad practice". The risk is revisited annually in January. This should remain on the Risk Register to prove to the FSA that we have taken this issue seriously yet retained the level of authentication due to the demographic of the customer base

19.7.4 POca as a product is contracted to run until 2015, any extension or replacement product must take account of the customer demographic and the difficulties in relation to customer authentication over the phone. E.g. use of masked passwords and requests to customer to authenticate by the provision of 3 characters or their password would be a mistake

19.8 Copy statement requests

Risk: (LOW) Availability

Impact: Customer experience; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

POL00393731

1. Requests from customers for copies of printed statements are handed off to Tier 2 from Tier 1. Although not strictly speaking a risk, this seems on the face of it an unnecessary process for little gain

Recommendations

19.8.1 Review the rationale that statement requests can only be performed by Tier 2, and if no obvious security or operational reason allow Tier 1 to make the requests

19.9 Disaster Recovery and Crisis Management

Risk: (MEDIUM) Integrity, Availability, Fraud

Impact: Financial (product profitability, business and agent debt); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There is a very good invocation plan in place to cater for telephony loss at different times of day. That said, there was an occasion during a telephony loss (August 5th 2011 - Q17288402) where Call Plan F wasn't put in place as quickly as it could have been. This risk is possibly still present. It might be also the case that due to the rarity of Call Plan invocation that other levels of invocation may not be fully known by those involved
2. Each component of POca end-to-end (from POca SEOCS receiving infrastructure) is proven annually for recovery following a disaster. There are scenarios though which are not fully rehearsed. For instance the invocation of Emergency payments due to full loss of Counter services or the link between Horizon and EBT. Although emergency payments of £20 are available to customers, if the ability to interrogate a customer account to ensure funds are available is lost for all, the next scenario is to provide an emergency payment and keep the card behind the counter. This has not been used since August 2004, and is not believed to have been migrated as a process from the old contract to new, so is not documented for future use. It might be the case that a customer would not bother to return for their card and just use the lost/stolen process to gain a replacement

Recommendations

POL00393731

19.9.1 A simulation and rehearsal of Call Plan F should be planned in to ensure that HP, POL Duty Manager (out of hours) and BT are all aware of their duties. The rehearsal must be fully documented

19.9.2 A rehearsal of every Call Plan scenario should also be considered which also should be fully documented resulting in easy to follow step-by-step guides

19.9.3 A review of the POca emergency payments scenarios should be performed to ensure that the processes are fit for purpose and doable in a crisis situation

19.9.4 A crisis management exercise should be planned to simulate specific events which DR tests do not prove

19.10 Cheque production processes

Risk: (LOW) Availability
Impact: Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There are two main processes for the production of cheques; 1. Partial Balance Release request by phone which initiates a cheque within x working days payable only to the PAH. 2. A written request from the PAH for a cheque to be produced. The consultant listened into a call from a UK prisoner who stated that the prison governor had authorised the POca balance to be released by cheque to the prison's account for provision of funds to the prisoner. This became a problem call in that the cheque had not been processed and he was told that it may be 28 days, and became irate and abusive.

Recommendations

19.10.1 HP should review the cheque request and production processes, specifically in relation to the long delay mentioned above in order to manage customer expectation and also reduce the chances of abuse to CSRs

19.11 PEGA CRM black screen

Risk: (LOW) Availability
Impact: Operational; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. During the review, a problem with PEGA presented itself on the Tier 2 CSR screen. During interrogation of an account with a lot of deposit/withdrawal activity the CSR's screen went black and required reloading. The CSR had seen this before but not reported it. In fact he had a second instance of PEGA

POL00393731

running so could switch easily. There is a risk that small faults, if not reported could become major and service impacting. Even small and niggley faults with IT systems should be reported when seen to prevent the possibility they will become more solid with wider impact.

Recommendations

19.11.1 CSRs should be encouraged to report all faults, however small and niggley in order to minimise the possibility that there might be something more major and potentially service impacting underlying the issue

19.12 Unprotected emails received from POL Security Investigations

Risk: (MEDIUM) Confidentiality

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The HP Case Management team are at times receiving emails which includes sensitive customer or corporate confidential information from individual POL Security investigators. The sending of email across the public internet which is not encrypted risks interception and compromise of contents.

Recommendations

19.12.1 All notifications from POL Security investigators which need to be sent to HP Case Management team must be routed to a single point of contact in POL for onward sending protected by PGP encryption

19.13 DPA Section 29 requests from police (plus other authorised bodies) and Freedom of Information requests

Risk: (MEDIUM) Confidentiality, Integrity

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. In support of criminal or missing person investigations, Police may request information from a POca. Section 29 of DPA 1998 allows for personal information to be sent for Criminal or Taxation purposes. However, there is a risk to the Post Office brand and its partners in that the information, albeit sent in encrypted form, once with the recipient, is out of our control. If the documentation was printed and subsequently found where it shouldn't be Post

POL00393731

Office would be in the firing line of the ICO rather than the recipient police force

2. All necessary POca documentation in support of a police request is screen dumped and pasted into a Microsoft Office document. It is possible to manipulate MS Office documents so the integrity of the information cannot be guaranteed
3. HP must also produce similar documentation in relation to Freedom of Information requests. If lost or compromised, these too may create adverse PR

Recommendations

19.13.1 Ensure the following text is included in every email in response to a police investigation "The information in the attachment(s) to this email is subject the requirements of the Data Protection Act 1998. Post Office Limited is therefore informing the authorised requestor of their responsibilities under the legislation to ensure that the information requested and received is used only for the purpose or purposes for which the request was made, and that the information must be protected from loss and/or compromise and/or misuse, and securely destroyed at such time as the need and purpose for the request has expired"

19.13.2 Although POca information in support of a police request is copied to MS Office documents, these must not be sent out, and should be converted to adobe acrobat .pdf documents with an indelible watermark naming the recipient, reference and date

19.13.3 For all non-POca requests from law enforcement agencies Post Office Security should adopt as best practice the processes which HP use to minimise fallout on the POL brand should Information be lost or treated badly by the recipient

19.13.4 The same controls should be applied to responses to Freedom of Information requests

19.14 Staff records

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. The HP Contact Centre Operations team have excellent staff records which follow the employee through their career and document key events. This provides a good record of career events such as promotion, maternity/paternity leave, and also the levels of privilege to a POca IT systems, and physical access rights (swipe card). This is not the case though for Swansea or

POL00393731

Washington staff, nor POca IT systems or database administrators. Although not seen as a major risk, recording the same information for all HP staff that have access to POca systems will be of benefit

Recommendations

19.14.1 HP should consider extending best practice by reuse of the Contact Centre Operations process for POca employee tracking

19.15 Vulnerability to phishing and spear-phishing attacks

Phishing emails are designed to fool users into clicking on a malicious link which could be designed to harvest personal and corporate logon credentials, bank details or other financial or personal information; this is the more modern form of Social Engineering attack. A more targeted act, referred to as Spear-Phishing is to focus on specific individuals within a company following an element of research, and to tailor the emails accordingly in order to dupe the recipient into visiting fake websites or activate malicious links which would unwittingly activate a malicious payload.

This kind of attack is very much on the increase with many companies behind the curve in terms of education and awareness campaigns. See the following Computer Weekly articles for more detail

[HYPERLINK "http://www.computerweekly.com/opinion/Dont-Get-Spiked-by-a-Spear-Phisher"]
[HYPERLINK "http://www.computerweekly.com/news/2240176040/UK-office-workers-swamped-with-phishing-emails-study-finds?utm_medium=EM&asrc=EM_EDA_20309056&utm_campaign=20130115_UK%20office%20workers%20swamped%20with%20phishing%20emails,%20study%20finds_&utm_source=EDA"]

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. **[HYPERLINK "http://en.wikipedia.org/wiki/Phishing%20"]** and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**, which led the firm to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"]**. This attack was followed by a **[HYPERLINK "http://www.infosecurity-**

POL00393731

magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"] which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain, but for all intents and purposes, the "mark" is sent an email, possibly from a seemingly reliable source (which has been previously compromised), with a malicious payload designed to harvest logon credentials and/or other corporate confidential information, which could lead to compromise of customer databases

Recommendations

19.15.1 ***Each firm and government department should consider its vulnerability to this kind of attack, the impact of loss and/or compromise, and the awareness of staff to the dangers. They must consider what steps can be taken to minimise the threat as part of their Information Security Awareness programmes. A good start will be to visit [HYPERLINK "http://www.antiphishing.org"] and download the report entitled "Phishing Activity Trends Report 1st Quarter 2012". Note that the headline states "Financial Services continued to be the most targeted industry sector in the first quarter of 2012. [p. 7]. It is also recommended that firms consider as part of their campaigns the deliberate and controlled targeting of key members of their own staff (and executives) in mock exercises by means of available tools, such as [HYPERLINK "http://www.phishme.com"]. This is an example not an endorsement of the company delivering this service***

Note: Since writing this report, HP has shown the Consultant a very good online education and awareness application to highlight the risks of phishing attacks which is used within their company but it is not known whether all staff close to POca have received the training.

POL00393731

20 Main Areas of Risk (JP Morgan Europe Limited)

20.1 Risks still to be addressed following Tandem hardware maintenance review

The following **(LOW)** risks are outstanding at the time of writing, and Post Office is awaiting a response

1. ***Review of whether the journey of failed media from Doxford and/or Wynyard to Basingstoke is necessary.***
   JPM response 04/02/2013: "Further discussions to take place with HP on this item"

2. ***Results of the backup tape audit when available.***
   JPM response 04/02/2013: "Draft tape audit report has been produced by HP. This draft report is currently being reviewed within HP"

3. ***Review of powerful super.tandem credential***
   JPM response 04/02/2013: "We are in the process of working with the security team on the review of SUPER.TANDEM access. Target completion for this activity, including implementation of recommendations is end of Q1"

4. ***Eight failed discs still with the forensic recovery firm plus forensic copies***
   JPM Response 04/02/2013: "Once approval and request for secure destruction is made, a copy of the destruction certificates will be provided"

20.2 Requirement for further assessment of the EBT service

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Although EBT and Tandem support has been included in this end-to-end review, and since the October major incident a targeted review of the new hardware support arrangements has been performed, the lack of control around support and maintenance may indicate that other areas might require some scrutiny to minimise further risk to all organisations.

Recommendations

POL00393731

20.2.1 It is recommended that a targeted EBT review be performed in order to ensure that there are no other as yet unidentified risks to the POca service. Moreover, it is further recommended that this be led by HP in that JP Morgan is their sub-contractor. The Post Office Information Security consultant should accompany HP on the review but on this occasion HP should lead

20.3 Possible Data Loss through email attachments

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Although unlikely, from the Consultant's investigations it might be possible for a JP Morgan employee to zip and encrypt customer or corporate confidential data and send out of the firm as an attachment, which may not be intercepted by their monitoring procedures, in that it is believed that the test is that data is encrypted. The specific risk therefore is that POca information could be compromised, but from a JP Morgan perspective all information accessible by a possible "rogue" employee could be at risk

Recommendations

20.3.1 It is recommended that JP Morgan test this possible risk of data loss via email attachment and if true consider appropriate additional controls

20.4 Vulnerability to phishing and spear-phishing attacks

Phishing emails are designed to fool users into clicking on a malicious link which could be designed to harvest personal and corporate logon credentials, bank details or other financial or personal information; this is the more modern form of Social Engineering attack. A more targeted act, referred to as Spear-Phishing is to focus on specific individuals within a company following an element of research, and to tailor the emails accordingly in order to dupe the recipient into visiting fake websites or activate malicious links which would unwittingly activate a malicious payload.

This kind of attack is very much on the increase with many companies behind the curve in terms of education and awareness campaigns. See the following Computer Weekly articles for more detail

[HYPERLINK "http://www.computerweekly.com/opinion/Dont-Get-Spiked-by-a-Spear-Phisher"]

POL00393731

POca end-to-end Information Security, Technology and Product Process Risk Review

[HYPERLINK "http://www.computerweekly.com/news/2240176040/UK-office-workers-swamped-with-phishing-emails-study-finds?utm_medium=EM&asrc=EM_EDA_20309056&utm_campaign=20130115_UK%20office%20workers%20swamped%20with%20phishing%20emails,%20study%20finds_&utm_source=EDA"]

Risk: (MEDIUM) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. **[HYPERLINK "http://en.wikipedia.org/wiki/Phishing%20"]** and **[HYPERLINK "http://searchsecurity.techtarget.com/definition/spear-phishing%20"]** attacks on businesses, especially in the security, military and financial arenas are not uncommon. Some firms have been seriously and embarrassingly compromised, including **[HYPERLINK "http://www.emc.com/security/index.htm"]**, which led the firm to **[HYPERLINK "http://www.bbc.co.uk/news/technology-13681566"].** This attack was followed by a **[HYPERLINK "http://www.infosecurity-magazine.com/view/18299/were-rsa-hackers-behind-lockheed-martin-breach/"]** which "may have been the main target". These events go to highlight the need to educate staff about the perils of phishing attacks. This risk is the same for all firms in the POca Supply chain, but for all intents and purposes, the "mark" is sent an email, possibly from a seemingly reliable source (which has been previously compromised), with a malicious payload designed to harvest logon credentials and/or other corporate confidential information, which could lead to compromise of customer databases

Recommendations

20.4.1 ***Each firm and government department should consider its vulnerability to this kind of attack, the impact of loss and/or compromise, and the awareness of staff to the dangers. They must consider what steps can be taken to minimise the threat as part of their Information Security Awareness programmes. A good start will be to visit [HYPERLINK "http://www.antiphishing.org"] and download the report entitled "Phishing Activity Trends Report 1st Quarter 2012". Note that the headline states "Financial Services continued to be the most targeted industry sector in the first quarter of 2012. [p. 7].*** **It is also recommended that firms consider as part of their campaigns the deliberate and controlled targeting of key members of their own staff (and executives) in mock exercises by means of available tools, such as [HYPERLINK "http://www.phishme.com"]. This is an example not an endorsement of the company delivering this service**

POL00393731

21 Main Areas of risk (HP IT systems)

Risk: (LOW) Confidentiality, Integrity, Availability, Competition

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Competitive; Customer and Shareholder confidence; Public relations; POCA partner Brand image.

21.1 HP SharePoint site access

1. HP provides access to POca technical documentation to staff and to partners via their SharePoint site. This site includes all POca technical documents (TED, PED, AIS, and TIS etc.). Although not likely, access is to a specific URL via username and password from any internet connected device. There is a risk that those with credentials could continue to use after leaving employment. This could be a PR risk in that open publication would be embarrassing. Moreover, these documents might be of interest to a competitor of POL or its partners

Recommendations

21.1.1 HP should review access credentials to this POca SharePoint site with their partners; the target being removal of any and all redundant users. Consideration to limiting access to customer sub-net IP addresses might also be considered

21.2 Data backups (generic risk)

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. At present backups taken from each of the POca IT systems are written to tapes in clear text. I.e. not encrypted. Although strict controls are in place to minimise any compromise of these tapes both whilst onsite within the data centres and offsite storage under the control of Iron Mountain, a small risk remains that these tapes, if compromised, could be read and copied

Recommendations

21.2.1 This is more for information only in that HP has a project underway for all POca systems to move to encrypted backups. As yet POL does not have a target date for deployment. Note though that there will be a substantial

POL00393731

number of existing unencrypted tapes which will need to be stored for ongoing legal and regulatory retention purposes

21.3 Database storage and media replacement (generic risk)

A **(CRITICAL)** risk was identified during the consultant's visit to the Doxford and Wynyard data centres in that it became evident that the SAN disc replacement process did not provide a full auditable chain of custody and likely included a journey, which although in engineers' cars, could not be deemed to be secure. Within a couple of hours of the risk identification HP agreed an immediate change which ensures that all discs that may contain POca data will be stored securely onsite until secure sanitisation/destruction processes have been agreed. This risk has therefore been downgraded to **(MEDIUM).** It is not possible to remove the risk completely until Post Office has seen the full process description that will ensure full chain of custody through to secure sanitisation or destruction.

It is important though to note that it is very unlikely that any POca data has been compromised in this way in that the SAN is shared (multi-occupancy) with POca data tables, like all other resident data spread over multiple discs. I.e. subject to "RAID" storage technology that combines multiple discs into a logical unit offering redundancy, so that if a disc fails no data is lost and the failed disc can be replaced "on the fly". The likelihood therefore of any failed disc containing complete records is slim. Moreover, although failed discs could contain POca data, they could equally contain other data. To contextualise this, the SAN in question is 200Tb, with POca data limited to 20xTb

A similar risk was identified within the JP Morgan space following an incident in October, but has been dealt with separately and is documented below in this report

Risk: (MEDIUM) Confidentiality

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; fines; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. There is a risk of data loss and/or compromise if processes for failed media replacement and media decommissioning are not communicated, followed, robust, repeatable and auditable with records that prove full chain of custody and secure sanitisation/destruction

Recommendations

21.3.1 HP to provide details proving full chain of custody and sanitisation/destruction for any and all media which has been replaced through fault or decommissioning over the past year. For the avoidance of doubt this is media that did or may have contained POca data, so for the

POL00393731

data centre SAN discs, this is from the date of migration, which is less than 12 months

21.3.2 HP to provide Post Office with a media replacement process map which provides a full auditable chain of custody and records of secure sanitisation/destruction, which must include:

- **engineer call**
- **onsite checks and authorisations**
- **removal of failed discs**
- **population of new disc including any engineer logon to the device and high-level credential use by the engineer or a remote procedure**
- **what happens to the failed disc**
  i. **journey**
  ii. **to where**
  iii. **what happens when received at destination**
  iv. **storage**
  v. **sanitisation**
  vi. **destruction**

21.3.3 POL to commission an audit, 6-months after agreement is reached that secure processes for media replacement/decommissioning have been agreed. This audit must to cover both HP and JP Morgan and prove that records exist, are accurate and prove that agreed process is being followed 100% of the time

21.3.4 POL and its POca partners must be constantly vigilant in minimising threats of external hacks or internal skulduggery. It must be noted though that HP has robust protection against external intrusion and tight access control and privilege management. All involved in the POca supply chain though should be fully aware that it is not possible to fully de-risk the chance of data loss or compromise as long as POca records are not encrypted at rest (on hard disc or backup tape)

21.4 Software and hardware support (generic risk)

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Although confidence is high in HP IT development and support staff, it is best practice to ensure that written code not only performs the function it is designed to do, but is also secure from bugs, back-doors or scripting errors which may not be obvious. Without strict secure coding techniques there is always the risk that software may be performing routines which were not part of the requirements, and at the extreme end of risk, that code might contain

POL00393731

accidental or malicious elements which might be exploited. Moreover, there are risks specific to operating systems, whether Windows, UNIX or LINUX, all of which are used for POca delivery which need to be considered

Recommendations

21.4.1 It is advised that secure coding standards and systems support include review against advice from the SANS organisation and OWASP (Open Web Application Security Project). See links

- **[HYPERLINK "https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project"]**
- **[HYPERLINK "http://cwe.mitre.org/top25/"]**
- **[HYPERLINK "http://www.sans.org/critical-security-controls/"]**

21.5 Software development and support (segregation of duties principle)

Risk: (LOW) Confidentiality, Integrity, Availability, Fraud

Impact: Financial (product profitability); marketability of future financial and banking products; Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA partner Brand image.

1. Although confidence is high in HP IT development and support staff, it is best practice to ensure that duties are segregated. I.e. development staff should not in theory have access credentials to both test and live environments. This does occur within HP POca teams, particularly the small team base in Milton Keynes. That said, we must all be aware that this is the case in most organisations. Full accountability is important, but the ability to trust staff is vital

Recommendations

21.5.1 None: for information only

21.6 SEOCS (DWP IT support and maintenance)

Risk: (MEDIUM) Confidentiality, Integrity, Availability

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

POL00393731

POca end-to-end Information Security, Technology and Product Process Risk Review

1. Following a SEOCS issue HP (POca) attempted to contact their opposite number in DWP (HP) to. It transpired that the support for the DWP side of SEOCS has transferred to ATOS/Accenture but they were unaware. There is a risk that partner and support provider changes which are not communicated will delay any incident resolutions, and could impact on operational continuity. There have been also some issues with Key Management procedures not being understood by the new provider
2. 1 above also creates the risk that customer personal information, subject to the principles of DPA 1998 may be available to ATOS/Accenture staff, and there may be remote diagnostic links which might provide an entry point if not adequately controlled. Although POca data on the government side is their responsibility, compromise or loss could generate adverse publicity for the product and therefore the Post Office

Recommendations

21.6.1 DWP should provide contact details for SEOCS support to enable swift incident response and resolution

21.6.2 DWP should satisfy itself that all necessary controls are in place to prevent ATOS/Accenture staff from having access to POca data should they not need it, and strict controls to prevent loss and/or compromise should they need access. This must include robust controls to ensure all accesses and any remote diagnostic links are fully monitored and auditable

21.6.3 DWP, POL and HP need to understand implications of the changes to SEOCS support from HP to ATOS/Accenture in relation to management of incidents, protection of personal data and encryption key management so that documents and processes can be updated to reflect the change. A meeting should be scheduled

21.7 SEOCS (lack of testing environment)

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Regulatory; Operational; Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. SEOCS does not have a test environment. This was a decision made at project stage. Cost would probably have been a factor. There remains though a risk that a change not thoroughly tested to UAT is applied to the live environment which is not "best practice" and could impact service.

Recommendations

POL00393731

21.7.1 None: For information only. Note that the DR environment exists so if problems with live does occur then a switch to DR can be made as long as the same code changed hasn't been applied to both instances

21.8 SEOCS (incident management POL and DWP)

Risk: (MEDIUM) Integrity, Availability

Impact: Regulatory; Operational; Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. There have been incidents where files have failed to be sent or where two files of the same name have been sent. E.g. incidents in 2012 dated 11 Aug, 13 Aug, 3 Sep, 11 Sep, 1 Nov, 3 Dec, 10 Dec. There doesn't seem to be any follow-up or trend analysis where SEOCS incidents are reviewed to minimise repeats

Recommendations

21.8.1 Post Office Service Desk should ensure that repeat incidents, in this case SEOCS, are the subject of trend analysis to identify repeats of the same kind in order to discuss with clients and partners ways to improve. DWP should consider a similar review of SEOCS incidents to identify improvement opportunities

21.9 CRM system

No CRM technology specific risks have been identified, but see Contact Centre risks above for some user risks

21.10 Tower system

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. The HP Tower system contains images of documents, letters and POca application forms, the latter which includes all customer application details including EVP questions and answers. Most access to Tower is performed via the PEGA system, but some staff have a need for direct access. Although the risk is low of any misuse, at the time of the review it wasn't known if audit trail of these accesses reports down to the level of which images have been viewed

POL00393731

Recommendations

21.10.1 HP should review audit capability on Tower to investigate if records of viewed documents are taken, and if not consider whether this might be introduced

22 Main Areas of risk (HP data centres)

22.1 Vehicle entry (Doxford) - tailgating

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. Automated gates allow vehicle entry to the Doxford data centre either by Swipe/PIN for authorised onsite staff or for authorised visitors by security staff using CCTV and voice communications with the driver. There is a risk, albeit LOW that a vehicle, and possibly two or three could tailgate the authorised vehicle before the gate would be shut. Although the risk is LOW, it must be borne in mind that the data centre delivers services to Post Office and other government departments, and is part of the UK CNI. It is not beyond the realms of plausibility that terrorists could see the site as a target for a truck bomb

Recommendations

22.1.1 HP should consider the implementation of a two-gate solution as they have in the truck entry at Wynyard. I.e. gate 2 does not open until gat 1 is closed

22.2 UPS Battery room (Wynyard)

Risk: (LOW) Availability

Impact: Regulatory; Operational; Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. One of the UPS battery rooms was visited and it was noticed that only one air-conditioning unit was in place to cool the room. There is a risk that this unit fails and batteries become overheated. Unless there is something which was missed at the time, this should be viewed as a single-point-of-failure

Recommendations

POL00393731

22.2.1 HP should review the risk of this device failing and if deemed necessary a second air-conditioning unit should be fitted

22.3 Visiting engineer vetting (both data centres)

Risk: (LOW) Confidentiality, Integrity, Availability

Impact: Regulatory; Operational; Criminal, Customer and Shareholder confidence; Public relations; POCA client, POL, partner Brand image.

1. Each and every member of staff who works in the data centres is vetted and cleared to the UK government's SC level. At the time of writing this report it is not clear whether visiting engineers who may be responsible hardware maintenance including the replacement of unencrypted data discs are vetted to a level required by the POca contract

Recommendations

22.3.1 Post Office requires that all those who come into contact with POca data, or who support POca systems are vetted to the level required by the contract between POL and HP. Confirmation is required.

23 Disaster Recovery

Full Disaster Recovery Capabilities are provided for POca systems and customer management. These are listed in the table below. Each element of Disaster recovery capability is tested annually with Post Office attendance and for which Post Office receives written reports

NOTE: It should be borne in mind that should DR be invoked for CRM, up to 15 minutes of in-flight data could be lost. I.e. could results in inconsistencies between CRM and EBT

Component	Prime Facility for "business as usual"	Backup Facility for DR
Contact Centre/ Back office function	The contact centre operation is in fact split over two sites, the Prime Contact Centre (Preston) hosting 95% of the front office seat capacity and the back office function, and a smaller contact centre located in HP Warrington. The out of hours Lost and stolen is handled out of either centre as appropriate	In the event of a disaster, the Warrington contact Centre provides immediate reduced capacity call facilities. (Lost and Stolen only) In addition, a specialist Contact Centre DR outsourcing agreement, provided by SunGard at

POL00393731

Component	Prime Facility for "business as usual"	Backup Facility for DR
		Warrington, has been put in place to provide temporary contact centre facilities up to full seat capacity.
Telephony	Prime telephony is provided from a leveraged service located at the HP Doxford Data centre.	DR Telephony is in multiple layers. There are layers of resilience built into the Prime system which cater for many scenarios but ultimate fallback will be to use a Local Survivability Processor (LSP) located in Preston or to invoke DR telephony at the DR contact centre in SunGard Warrington.
Scanning	The Prime scanning facility is located at a dedicated scanning site in Swansea.	Backup Scanning facilities is provided at the DR contact centre in SunGard Warrington as above.
Document Repository	The Prime Document repository is located in the HP Doxford Data Centre. This allows rapid access to the image repository from the CRM system.	Backup document repository facilities are provided at the HP Wynyard Data Centre.
AVS	The Prime AVS system runs on a server located in the HP Doxford Data centre, co-hosted on the Prime CRM system.	The DR AVS system is provided at the HP Wynyard Data Centre, co-hosted on the DR CRM system.
EBT	The Prime EBT system is located in the HP Doxford Data Centre.	DR EBT facilities are provided from the provided at the HP Wynyard Data Centre. Doxford and Wynyard are linked by dual resilient fibres to allow EBT to synchronise the data between live and DR.
Message Broker	The Prime Message Broker is co-located with the Prime EBT system. This is to facilitate LAN speed communications between them.	Backup message broker is co-located with the DR EBT system.
CRM system	The Prime CRM system is provided at the HP Doxford Data Centre.	The DR CRM system is provided at the HP Wynyard Data Centre.
Fulfilment – Bulk Printing	The Prime Fulfilment centre for printing is at the HP Washington OSSG print centre.	The Backup Fulfilment centre for printing is the HP Norcross OSSG print centre.

POL00393731

Component	Prime Facility for "business as usual"	Backup Facility for DR
Cheque printing system	The Prime cheque printing process is managed and fulfilled provided by a third party supplier to JP Morgan	Also provided by a third party supplier to JP Morgan.
BACS	The Prime BACS connectivity is via the JP Morgan data centre connectivity co-located with the Prime EBT system.	The DR BACS connectivity is via the JP Morgan data centre connectivity co-located with the Backup EBT system.
Faster Payments Service*	The Prime FPS connectivity is via the JP Morgan data centre connectivity co-located with the Prime EBT system.	The DR FPS connectivity is via the JP Morgan data centre connectivity co-located with the Backup EBT system.
NBX (Out of Scope)	NBX consists of two pairs of servers mirrored across two sites. These sites are the Fujitsu Data Centres, both located in Belfast albeit with a healthy geographical distance between.	No DR Facilities are required as this service operates in a Live/Live mode.
ATM	The Prime ATM connectivity is via the JP Morgan data centre connectivity co-located with the Prime EBT system.	The DR ATM connectivity is via the JP Morgan data centre connectivity co-located with the Backup EBT system.
SEOCS	The Prime Microsoft (MS) Exchange and PGP installation is located at Doxford. The Message Processing aspects run on the Prime CRM system, located in the HP Doxford Data centre, co-hosted on the Prime CRM system.	The backup for the MS Exchange and PGP server installations is provided at the HP Wynyard Data Centre The Message Processing aspects run on the DR CRM system located at the HP Wynyard Data Centre

24 Application and (other) forms rejections

Observation of paper document check and send was not possible during Crown Office visits in that none were presented during the time the Consultant was present. However, the visit to the HP Input Capture Centre was fruitful. Much time was spent witnessing the receipt, batching, sorting, scanning, processing, secure storage through to the dropping of a full days' paper into sensitive waste destruction bins after one calendar month.

There are issues relating to the rejection of POca applications and other forms. These are detailed below with some recommendations for improvement which should be considered.

POL00393731

THIS PAGE BLANK TO ENABLE CHANGE OF ORIENTATION

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

Issue no	Form number	Purpose	Common mistake/Issue	Impact	Improvement recommendation (POL)	Improvement recommendation (HP)
1	**P6629**	Application form	FAD Code missing	Rejected to customer	Reiterate message to all outlets that FAD code omission is a problem and that missing codes means that no remuneration will be issued for application check and send	Do not reject application where FAD code missing. NB. A solution will be required for an acceptable FAD replacement so as not to impact SLA. E.g. FAD = 1111111
2	**P6629**	Application form	In "office use only" section: Date mismatch between stamp and date entry. Instruction to HP is take the date of the stamp before entered date. However, stamp date sometimes unreadable and entered date obviously wrong	Affects SLA account opening target	Reiterate message that date stamp should be clear and readable and that written date should be "today"	None

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

3	**P6629**	Application form	Some names entered on pre-populated form at DWP level do not always match the name on the ID even though it is the same person. Particularly problematic with foreign names. E.g. forename = Ali, family name = Abu-Shah may be the name the customer presents ID with, but the P6629 name pre-populated by DWP may say only forename = Abu, family name = Shah	Rejected to customer	Reiterate to Post Office staff that where the name on the presented ID does not absolutely match the name on the P6629 to inform the applicant that the form cannot be processed and to return to the issuing authority for a replacement. **Inform DWP that this is an issue and that their clerks should take extra care to ensure that the name entered is the real full name of the applicant and recorded as it appears on the ID the customer will be presenting at the counter**	None
4	**P6629**	Application form	It is obvious from the difference between the stamp dates and the dates received in Swansea that some Post Offices are hanging onto application forms and other POca forms rather than sending each day (except Saturday)	Affects SLA account opening target	Reiterate to Post Office staff that all POca forms must be despatched daily (except Saturdays) in the P6224 envelope, which must be placed into the Orange & White daily despatch pouch (ENV2062) with the address of Post Office Processing Department, IPSL, Blaise Pascal House, 100 Pavilion Drive, Northampton. NN4 7YP. This is the only allowable method of despatch. Do not post POca forms via Royal Mail.	None

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

5	**P6363**	Evidence of identity	Where two forms of identity have been presented to accompany an application, and both have been recorded, it is often the case that one is entered correctly and the other not	Rejected to customer (application or form) with the words "the name we have recorded from your identification does not match the name on your application form". Note that this is not correct in that one form of ID was acceptable, and this message tends to confuse the customer, which leads to a second application rejection	Reiterate to Post Office staff that only one form of identification is required to open a POca and that accuracy of entry is imperative	Do not reject application where one form of identification is recorded correctly, even if a second has not been

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

6	**P6363**	Evidence of identity	It is often the case that even though identity documentation has been seen and recorded correctly, the "ID Item" field has not been recorded	Rejected to customer (application or form)	Reiterate to Post Office staff the need for accuracy on the P6363 and to ensure that the "ID Item" number is always recorded	Where there is an obvious record of a known form of identity. E.g. PAN or credit/debit card, Driving Licence number then enter the appropriate "ID Item" number to prevent rejection. This recommendation should be approved by JP Morgan and not impact productivity adversely

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

7	**P6363**	Evidence of identity	Married women are often disadvantaged when applying for a POca if they present their Birth Certificate in that the maiden name on the document is not the same as their married name. The wording on the P6363 is for the clerk to record the "name on the document", so it is correct to do so.	Rejected to customer (application or form) with the words "the name we have recorded from your identification does not match the name on your application form", causing confusion in that they have shown ID as required	Inform Post Office staff that forms of identification presented in support of an application or form **must** be in the same name as the applicant. Therefore, where a customer (in particular, a married woman) presents a birth certificate where the family name is different to applicant name then please ask the customer to present a form of acceptable ID (from the list) where the names match. Otherwise the application (or form) will be rejected	None
8	**P6363**	Evidence of identity	General accuracy of the P6363 is affecting customers detrimentally. In particular, customer names can be written wrongly on the evidence of identity form. When this occurs the application or associated form will be rejected	Rejected to customer (application or form)	Inform Post Office staff that inaccurately completed P6363 forms will lead to applications and forms being rejected adversely affecting POca customers	None

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

9	**P6363**	Evidence of identity	The P6363 form does not always accompany an application	Rejected to customer	Inform Post Office staff that POca applications (and other forms where ID must be proven) must be accompanied by a P6363, otherwise the application is rejected and the customer suffers delay	None
10	**Various original ID documents**	Evidence of identity original documentation presented at the counter	HP is receiving some original forms of identification which they have to apply a duty of care to and return to the customer. Although much of this tends to come direct from customers some is being sent from post Office outlets	HP must return items to customer, and where high-value items (e.g. passports/driving licences) have been sent they are returned "special delivery". This is a risk to the customer and also a PR risk to POL and HP should items go missing or be intercepted	Reiterate to Post Office staff that there **is never** an occasion where an original document is to be sent to HP. The majority of transactions require only the certified recording that a valid form of identity has been presented. For "change of name", "deceased account form" and "appointed legal representative" is it necessary for the clerk to see and record an original "deed poll", Marriage Certificate", "death certificate", "power of attorney" or "court order". **The original of any and all of these documents must always be returned to the customer and only a photocopy sent to HP for scanning.**	None

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

11	**Window Banker envelopes**	customer communications from both Swansea and Washington	Position of envelope window from Swansea is upper left quadrant, whereas Washington is central. "Gone Aways", i.e. envelopes returned to sender, arrive in Swansea for scanning of envelope address followed by unopened secure destruction. As their "duty of care" HP Swansea is able to identify envelopes sent by themselves. I.e. where "originals" have been returned as "gone away".	The ability to identify communications from Swansea enables staff to pull out their own mail for further investigation, which enhances the POca "duty of care"	None	Unless there is a good reason to change, ensure that the envelopes used in Swansea are identifiable from those used in Washington

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

12	**Cheques**		Cheques sent for account closure that are returned to sender as "gone-aways" can be identified by the colour of the paper through the window banker and can therefore be pulled out for further investigation rather than being scanned and destroyed	The ability to identify cheques from the envelope window enables Swansea enables staff to pull out for further investigation, which enhances the POca "duty of care"	None	Unless there is a good reason to change, ensure that cheques continue to be identifiable through the envelope window

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

13	**P6164**	Deceased Account form	This form cannot be processed without the presence of the "indemnifier's" signature if the account has a balance. Many deceased notifications are received with only the "representative's" details. Note that the Horizon online help states: "*The Deceased Account form P6164 can be used in two ways. A representative of the indemnifier may complete sections 1, 2 and 3 and report a death of an account holder or an indemnifier can complete sections 1, 2, 3 and 4 and can then claim the funds*".	The form is rejected back to the PAH, who of course is deceased, thereby creating additional stress and anxiety on friends and relatives during a time of bereavement	Reword the Horizon Help screen to the effect that although Sections 1,2 and 3 may be filled in by a representative of the indemnifier, Section 4 must be filled in by the indemnifier where the account is in credit. I.e. the representative may be the same person as the indemnifier or different, but Section 4 must be completed if the form is to be accepted. Send interim instruction to Post Office staff never to accept a P6164 form which has not had Section 4 completed overleaf. **This is mandatory.**	None
14	**P6167**	Card Account Closure form	This form can be processed by presentation at the counter without any form of identity check, and will be processed purely on signature validation by a CSR	The lack of face-to-face identity check is a facilitator for fraud, and has been misused in the past where the signature was forged	Serious consideration should be given to the introduction of a face-to-face identity check at the counter to ensure that the persons presenting with account closure and residual funds transfer request is the Primary Account Holder	None

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

15	**P6224**	**Pouches**	Some POca pouches are received in Swansea with other non-POca forms and documents. This is a non-conformance issue. HP send all non-POca documentation to Future Walk, Chesterfield	Delays in processing for other products	General notice to all outlets. "The P6224 POca pouch must not be used for anything except POca paper documentation and forms. If you have forms or documents for other products which you are unsure how to deal with, call NBSC on xxxxxxxxx"	

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

16	**14E**	Rejection letter	The 14E rejection letter responses are based on the embedded "CMS Decisioning" document below.	The responses back to the PAH do not always present the reality of the rejection. E.g. where one form of ID is good and the other not the response is still "our records show that we have either not received details of any proof of identification or the details we received are incomplete ". The same applies when the counter clerk has not completed "ID item" number. The response does not guide either the PAH or the Counter Clerk to the real rejection reason in many instances	Review these reject responses with HP and agree options for improvements to both minimise further rejections and enhance customer experience. This may already be underway as part of the improvements project being led by Nick Grace (HP)	Work with Post Office to agree possible improvements

POL00393731

POST OFFICE LIMITED CONFIDENTIAL

POca end-to-end Information Security, Technology and Product Process Risk Review

17	**NONE**	HP Decisioning response options	 CMS Decisioning.xls			
19	**NONE**	General issues	Two of the main reasons why applications and other forms are rejected is the lack of either a signature or a date, or both	Rejection to customer	Reiterate to Counter staff the importance checking all POca forms thoroughly before accepting for processing	None

POL00393731

THIS PAGE BLANK TO ENABLE CHANGE OF ORIENTATION

POL00393731

25 Requirement for further work

25.1 JP Morgan and EBT additional review

The review of the JP Morgan EBT system at the application level was performed in advance of the physical reviews of the Data Centres at the infrastructure level, and in advance of a major incident discovered in October 2012. Since that date a targeted review of the EBT hardware maintenance contract has been performed and the consultant has reported satisfaction with the new contractor and processes, notwithstanding some minor risks.

There have other audits since that time, so additional work during the end-to-end review would probably not have been easy. However, it is recommended that a targeted EBT review be performed in order to ensure that there are no other as yet unidentified risks to the POca service. Moreover, it is further recommended that this be led by HP in that JP Morgan is their sub-contractor. The Post Office Information Security consultant should accompany HP on the review but on this occasion HP should lead

See embedded documents: Risk Analysis or Tandem hardware maintenance contract and associated executive summary


RA JPM Tandem EBT break fix contract - n


exec summary RA Tandem EBT Break fix

25.2 ATM Integrity Review

It is recommended that ATM use and associated Management Information is assessed for accuracy; in particular but not limited to dispensed values and cash holdings plus fraud monitoring and reporting

25.3 Out of course documentation

There are both Information Security and service level implications which need to be reviewed due to the fact that pouches are routed through (IPSL) Intelligent Processing Solutions Ltd (**[HYPERLINK "http://www.ipsl.co.uk/index.html"]**), and that "out of course" documentation is sometimes not protected by tamper evident envelopes. It is therefore recommended that an onsite review is performed of the receipt, management and onward transmission of any and all POca paper documents, plus any other Post Office documents. The main objective of this review will be to minimise

POL00393731

compromise or loss of customer personal information; secondary will be to improve POca Service Level target achievement, particularly for new application processing.

25.4 Cheque printing

JP Morgan employs a third party company; Bottomline to print POca cheques and Data Graphics provide Disaster Recovery capability. The cheque production process and the two firms involved have not been reviewed as part of this exercise. It recommended they are in the near future.

26 References

26.1 Interviewees

Thanks go to the following people who attended meetings or were spoken to by phone:

Crown Offices

Bev Robinson	POL – Branch Manager (Leeds Crossgates)
Sharon Ewart	POL – Branch Manager (Leeds Markets)

HP Swansea

Leigh Gough	HP - Input Capture Centre manager
Mark Geldart	HP - Production Support/Security Manager
Ross Craig	HP - Service Delivery Executive

HP Washington

Alan Siddell	HP - Production Manager
Karen Laws	HP - Quality Manager
Norman King	HP - Account Delivery Executive

HP Preston

Mark Geldart	HP - Production Support/Security Manager
Ross Craig	HP - Service Delivery Executive
Susan Burgess	HP - Admin to SDE
Dave Solkin	HP - Contact Centre Operations Manager
Helen Wilson	HP – Helen Wilson – Call Centre Manager
Natalie Mitchell	HP - Tier 1 CSR
Andy Gibbons	HP - Tier 2 CSR
Katie Murray	HP - Case Management
Ashleigh Alston	HP - Case Management
Jacqui Wilkinson	HP - Training and Quality Coordinator

HP Data Centres

Gillian Avis	HP - Northern Region Data Centre Manager

POL00393731

Rob Donmell	HP -	Data Centre Operations Manager
Steve Hutchings	HP -	Account Delivery Manager
Bob Shonewald	ISS -	Facilities Manager

JP Morgan (Europe) Limited

Spencer Chartres	JPM -	POca Product Manager
David Wrigglesworth	JPM -	POca Product Specialist
Lenka Lukacova	JPM -	POca Product Analyst
Derek Smallworth	JPM -	POca Technology Manager
Brian Maskall	JPM -	POca Technology Manager
Dominic Aitken	JPM -	POca Technology Analyst

26.2 POca lifecycle

POCA-0651 POCA lifecycle v3 1.pdf

26.3 POca Security Plan

Post Office Card Account Security Plar

26.4 High Level System Flow diagram

ASFO-EMEA-POCA-0201 POCA System Flc

26.5 HP ISO27001: 2005

HP ISO27001 2012 - 2013 certificate.pdf