

**FUJITSU RESTRICTED**

Document Title: 2015 POA Problem Management – Problem Review

Document Reference: SVM/SDM/INR/3037

Release: Release Independent

Abstract: This report contains the trend analysis of the 34 problem records raised in the POA Problem Management TfS database during 2015.

Document Status: For Review

Author & Dept: Jolene Ngu – Problem and Major Incident Management

External Distribution: Not Applicable

Security Risk Assessment Confirmed Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

Approval Authorities:

Name	Role	
Steve Bansal	Senior Service Delivery Manager	

See RMG BU Reviewers/Approvers Matrix (PGM/DCM/ION/0001) for guidance on who should approve.



0 Document Control

0.1 Table of Contents

0	DOCUMENT CONTROL.....	2
0.1	Table of Contents.....	2
0.2	Document History.....	2
0.3	Review Details.....	2
0.4	Associated Documents (Internal & External).....	3
0.5	Abbreviations.....	4
0.6	Glossary.....	4
0.7	Changes Expected.....	5
0.8	Accuracy.....	5
0.9	Security Risk Assessment.....	5
1	INTRODUCTION.....	6
2	ANALYSIS.....	6
2.1	Categorisation.....	6
2.2	POA Review of Problems in the Fujitsu Domain or Further Consideration Required.....	6
2.3	Table of Results.....	7

0.2 Document History

Only integer versions are authorised for development.

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	05/01/2016	Initial Draft – This version was used for the formal 2015 Problem review held on Wednesday 20 th January 2016.	
0.2	21/01/2016	Second draft containing updates following the formal 2015 Problem review held on Wednesday 20 th January 2016.	
0.3	03/05/2106	Revised to include updates on closed Problem Records and providing feedback on actions	

0.3 Review Details

Review Comments by:	
Review Comments to:	Jolene.Ngu GRO + RMGA Document Management

If preferred you can delete the following Mandatory and Optional reviewer tables and paste in the appropriate list copied from RMB BU Reviewers/Approvers Matrix (PGM/DCM/ION/0001).

Mandatory Review	
Role	Name



Senior Service Delivery Manager	Steven Bansal
---------------------------------	---------------

Optional Review	
Role	Name
Problem Manager	Steve Gardiner
Remote Infrastructure Management	Rajaram Kuppuramaseshan
Systems Management & Global Cloud Manager	Catherine Obeng
Service Delivery Manager	Roger Stearn
Infrastructure Manager	Andy Hemingway
Chief Architect	Torstein Godeseth
System Architect	Mia Angell
Test Manager	Mark Ascott
Service Delivery Manager	Yannis Symvoulidis
SAP Service Delivery Manager	Paul Mailey
Principal Technical Services Specialist	Neil Preston
Principal Technical Services Specialist	Andrew Gibson
Senior Customer Solutions Architect	John Bradley
Head of Post Office Transformation Service	Iain Janssens
Senior Project Manager	Katy Hogan

(*) = Reviewers that returned comments

Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
POA Operations Director	Peter Thompson

0.4 Associated Documents (Internal & External)

References should normally refer to the latest approved version in Dimensions; only refer to a specific version if necessary.

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)	See note above	See note above	RMGA BU Generic Document Template	Dimensions
PGM/DCM/ION/0001 (DO NOT REMOVE)			RMG BU Document Reviewers/Approvers Role Matrix	Dimensions
SVM/SDM/PRO/0025			POA Problem Management Procedure	Dimensions

0.5 Abbreviations

©Copyright Fujitsu Limited 2016

FUJITSU RESTRICTED

UNCONTROLLED WHEN PRINTED OR
STORED OUTSIDE DIMENSIONS

Ref: SVM/SDM/INR/3037
Version: 0.3
Date: 03-May -2016
Page No: 3 of 17



Abbreviation	Definition
ADSL	Asymmetric Digital Subscriber Line
AP	Automated Payment
BAL	Branch Access Layer
BAU	Business As Usual
DVLA	Department of Vehicle Licensing Authority
GWS	Generic Web Server
ISP	Internet Service Provider
ITG	Information Technology Group (within Fujitsu Services)
KEL	Knowledge Entry Log
MCCB	Moulded Case Circuit Breakers
MSC	Managed Service Change
MSS	Managed System Service
NBSC	Network Business Support Centre
PM	Post Master
POA	Post Office Account
RCA	Root Cause Analysis
SSC	Software Support Centre (third line application support)
TfS	Triole for Service

0.6 Glossary

Term	Definition
PPD	Platform Physical Design
HDCR	Horizon Data Centre Refresh
NNM	Network Node Manager



0.7 Changes Expected

Changes

0.8 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.9 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.



Introduction

Within SVM/SDM/PRO/0025 the POA Problem Management Procedure there is a requirement in section 4.3 to undertake trend analysis, within section 4.4.2 to review the Knowledge database and within section 4.5 to review the problems which were raised, their ownership and continue monitoring for service improvement opportunities.

1 Analysis

This document contains the analysis of the 34 problem records raised in the POA Problem Management TfS database during 2015.

1.1 Categorisation

The analysis has been conducted in two phases. The first phase has been conducted by a POA Problem Manager and has resulted in categorising the problems into three types.

Type 1 – Further analysis is required within Post Office Account seeking input from POA design, development, testing and release. Sixteen problem records were classified under this category.

Type 2 – These were Administration Closures, e.g., the problem record was raised in error against the incorrect resolver group. Four problem records were classified under this Category.

Type 3 – The underlying issue was found to have originated in a third party domain, e.g., Post Office Limited or one of their clients or suppliers. Fourteen problem records were classified under this category.

1.2 POA Review of Problems in the Fujitsu Domain or Further Consideration Required.

On Wednesday 20th January 2016 at 09:30 a review was held of the problem records from 2015 which were categorised as type 1 by the following group;

Mark Ascott	Live System Test
Andrew Gibson	UNIX
Andy Hemingway	Infrastructure
Tony Wicks	Problem Management
Rajaram Kuppuramaseshan	SMC
Nirupama Sane	POLSAP Support
Gaby Reynolds	Online Services
Nick Crow	Branch and Comms Management
Jolene Ngu	Problem Management

Subsequent to the review applicable Problem Records for 2015 were discussed with Roger Stearn POA Networks SDM and Torstein Godeseth POA Chief Architect.

**FUJITSU RESTRICTED**

For each Problem Records of this type I have included a two further lines within the table documenting the findings and recommendations from the review or subsequent discussions, and proposed actions. It is planned that a follow-up on those actions will be conducted after 3 months – End of March 2016.

1.3 Table of Results.

<u>Problem Ref</u>	<u>Summary</u>	<u>Description</u>	<u>Proposed Action</u>	<u>Closed</u>
Problems in the Fujitsu Domain or Further Consideration Required.				
A10972720	The SMC site in Bangalore have been experiencing power loss and previous incidents indicate that it did not switch over to the emergency generator.	After carrying out a root cause analysis, it was ascertained that the failures were due to malfunction of the MCCB. The existing MCCB was replaced with a new MCCB and it has been tested on 4 cycles and no trip in current occurred.	Consideration should be given for the SMC to liaise with supplier of MCCB device to see if they can improve the quality of the delivered item.	Yes
<u>Findings and Recommendations.</u> A monthly check has been put in place to assist in preventing this from reoccurring in the future. The SMC has been monitoring for 2 months and no issue has been identified.				
<u>Action:</u> As a monthly checklist has been put in place, no further action is recommended.				
A10893754	System monitoring is falsely alerting that Reconciliation file transfers have abended and failed.	A master PEAK (PC0247384) was used to investigate the underlying fault and a fix has been targeted for Release 13.11 which is expected to be released to live in June 2016.	As a preventive measure, future designs checks can be done during development so false alerts won't occur during the releases.	No
<u>Findings and Recommendations.</u> At the review, it was agreed that coding checks could possibly be undertaken by Development.				
<u>Action:</u> Tony Wicks to write to Development requesting them to consider if it's possible to do some coding checks for this and similar situations as per the failure. This request has been made for Development's consideration.				
A10821106	Transaction discrepancies can occur during the Rem In process – especially when transferring cash	The underlying cause of this problem is that a logout before a user has fully logged on, then subsequently a pouch is rem-in manually, then after the rem in slip has been printed,	It is suggested that a 'regression' test for this type of failure could be run on new releases before released into the Live environment.	Yes

**FUJITSU RESTRICTED**

	from one branch to another (e.g., between their main branch to their outreach branch).	the same screen is redisplayed and if the user press Enter again, a duplicate will occur. A code fix has been developed and is in release 12.88 Hot fix		
<u>Findings and Recommendations.</u> It is suggested that a 'regression' test for this type of failure could be run on new releases before being released into the Live environment. A regression test has been added to the LST test suite to validate for this scenario in future releases.				
<u>Action:</u> As a regression test has been put in place since R12.88, no further action is recommended.				
A10530531	Network instability has caused a number disruptions to Post Office branch service during the week commencing Monday 12th October.	Specific targeted network traffic from a third party caused instability in the Fujitsu shared network. This irregular targeted traffic was caused by a configuration issue on a third party router.	Consideration should be given for Fujitsu Networks & Telecoms when implementing a new solution to protect the Fujitsu connect DSL network from abnormal traffic.	Yes
<u>Findings and Recommendations.</u> Fujitsu Networks & Telecoms advised a script was introduced during the Major Incident to protect the Fujitsu shared DSL network from a reoccurrence in the future.				
<u>Action:</u> No further POA / Fujitsu action is recommended.				
A10122010	VPX servers crashing.	<p>There are several underlying causes for the VPX crashes. Development have ascertain that it may be caused by memory leakage, NetCool probes or Server software upgrades including security patches.</p> <p>The POA Problem and Incident Team will be monitoring this until mid-February 2016 and Development will be following up on the NetCool concerns with MSS via PEAK.</p>	Consideration could be given for hardware and software upgrade based on the server lifespan.	Yes
<u>Findings and Recommendations.</u> NetCool Probe restarts are performed every day and will be monitored for the next 3 months. VPN has been added into Post Office Detail Branch Report. Additional measures have also been taken to monitor the VPX servers and entries are made into the report when there is a failure.				

**FUJITSU RESTRICTED**Action:

Investigations into this open Problem Record are on-going.

A9391723	Concerns have been raised within POA that there are possible SPoF within the HNG-X infrastructure and that a platform recovery strategy needs defining.	The POA Chief Architect was leading on the platform recovery strategy. Additionally, an exercise was started for Problem Management to liaise with the Disaster Recovery (System Owner) on the documentation that already exists on Single Points of Failure. SPOFs related to the BladeFrame will be going as part of Horizon Refresh.	There should always be a clear recovery strategy and capability defined for all platforms and a nominated owner for all platforms.	No
----------	---	---	--	----

Findings and Recommendations.

As part of the HNG-X Data Centre Refresh it is intended that Physical Platform Design specifications are being updated to include the platform recovery strategy within the document.

Additionally, a tactical solution is being implemented, under CP1725, for the cloning of platforms.

Action:

No further POA action to that above is recommended.

A9331408	POA are non-compliant with the ITG code of connection regarding Windows 2003 servers	POA are non-compliant with the ITG code of connection regarding Windows 2003 servers. There are three POA servers (LSBPPRG001, CITPXCS002, CITPNAL002) which ITG intend to quarantine on Friday 17th July 2015 and it is possible that there could be more servers. Tracking the project weekly ensured that all servers were migrated or retired with the exception of the Integration managed Dimension Servers.	Consideration should be given to always ensure that the operating system used is still in support and whenever necessary, for an update to be done before expiry date. If the operating system support is going to be withdrawn, an action needs to be taken before 1 year of the date.	Yes
----------	--	---	---	-----

Findings and Recommendations.

It was concluded that all servers should have proper design documentation, e.g., PPD's, regardless of whether in live or ITG.

Actions:

Tony Wicks to write to John Bradley highlighting the issue and requesting that consideration is given to documenting within the PPD's when the server and software support expires and constructing a database which contains component details & expiry dates and provides adequate advanced warning that support is going to expire.

**FUJITSU RESTRICTED**

Following discussion with Kate Hogan the recommendation is going to be considered by Development as part of the HDCR programme.

A9157908	Following GoldenGate replication aborting Branches reported cash declaration and stock reporting discrepancies 5th June 2015.	The underlying cause is the replication between GoldenGate and Oracle 10g and 11g aborted, resulting in a number of branches reporting cash declaration and stock reporting discrepancies.	Test team could consider if further tests could be carried out before releasing into Live.	Yes
----------	---	--	--	-----

Findings and Recommendations

The Live System Test team reviewed and considered the suggestion proposed by POA Problem Management and concluded that the time and effort required for the additional testing for irregular upgrades e.g., Oracle upgrade releases, was not justified.

Action:

No further POA action is recommended.

A9157767	Whilst applying Support Packs & Kernel Patches for POLSAP not all patches would load and short dump errors were seen 14th June 2015	Several underlying causes have been identified. The underlying causes identified were, changes and replacements to system solutions that integrate with POLSAP, other suppliers to Post Office of components that integrate or use POLSAP may be changed without detailed discussions or fully exploring the impacts, MSC 043J0436836 raised for corrective actions	Consideration could be given for improvement in test strategies in situations with multiple suppliers.	Yes
----------	---	--	--	-----

Findings and Recommendations.

It was concluded that this was due to unannounced changes in the third party domain. As this is outside of POA and Fujitsu control and POA Problem Management have already raised a cross domain Problem Record A9129261, "Unannounced and uncoordinated infrastructure changes are being implemented in third party domains which have caused serious service outages", for which ATOS Problem Management advised that ATOS are managing this under Continual Service Improvement 3893, no further action was identified.

Action:

No further POA action is recommended.

A8954715	An incomplete GlobalPay payment file was delivered on Wednesday 27th May 2015.	It was identified that the cause of the problem was a number of records that had not been removed from a database table by the standard housekeeping	As a corrective action has been put in place with 2 new columns added for housekeeping routines and a dashboard has been added to HORice, I do not	Yes
----------	--	--	--	-----

**FUJITSU RESTRICTED**

		<p>routines. These records have a primary key on them to identify the transaction to which they relate. The key is a 9-digit sequence number generated by the system and is recycled.</p> <p>Several corrective actions had taken place to resolve the problem. These actions are tracked under Major Incident Report Global Pay.</p>	<p>have a proposed action as this Problem Record was raised for the purpose of tracking actions.</p>	
<p><u>Findings and Recommendations.</u></p> <p>As a permanent corrective action has been put in place with 2 new columns added for housekeeping routines and a reporting capability for payment files has been added to HORice it was concluded that no further action is required.</p>				
<p><u>Action:</u></p> <p>No further action is required as the corrective action mentioned above has been completed.</p>				
A8721041	Post Code Anywhere – Request From Post Code Anywhere to update the Secure Socket Level Network Software.	POA Development undertook testing from a Development environment with PostCode Anywhere (PCA) as part of the Study which was conducted under CP1603. This conclude that no specific change was required. A fix took place which consist of two parts which are detailed in MSCs 043J0439149 & 043J0439154. Testing took place at the Post Office Model office which was deemed successful. MSC 043J0439154 took place and removed the static IP addresses.	I don't think that we could prevent a recurrence of this, i.e., Post Code Anywhere updating SSL network software is outside our control – but as a preventative measure this should be reported through the Network Service Reviews.	Yes
<p><u>Findings and Recommendations.</u></p> <p>There is no action that Fujitsu can take. POL and Atos should advise Fujitsu of any proposed changes in another domain. A Change Request should have been submitted by POL / ATOS. The related Problem Record is A9129261 and ATOS advised that they have raised a CSI 3893 to address the issue of unannounced and uncoordinated infrastructure changes being implemented by third parties.</p>				
<p><u>Action:</u></p> <p>No further POA action can be taken.</p>				
A8199235	Counters have crashed whilst	The underlying cause of the issue is an error in the coding	PC0241242 Consideration Could be	Yes

**FUJITSU RESTRICTED**

	performing Health Lottery Transactions.	for counter.	given for checks to be done for other all transactions types. If the transaction fails due to poor communication with the data centre (Network issue) and user was logged out by the system. When the user logged back in, the recovery kicked-in. But the recovery of transaction failed. (Test the recovery)	
<u>Findings and Recommendations.</u> <p>The Live System Test team reviewed and considered including this in the regression suite. However, this additional testing would require a considerable amount of manual input and resources. As this would extend the time period required for conducting the tests it was concluded that this additional regression testing could not be justified.</p>				
<u>Action:</u> <p>At this time no further POA action is recommended.</p>				
A7964442	The Foundstone Servers have not been fully operable following a recent upgrade	The core issue is that both Foundstone servers are broken and we are unable to get support from the vendor (McAfee) because both the hardware and software is end of life and our existing support contract expired 11-FEB-2015.	Consideration could be given to always ensure that the hardware used is still in support and whenever necessary, for an upgrade to be done before expiry date. If the hardware support is going to be withdrawn, an action needs to be taken before 1 year of the date.	No
<u>Findings and Recommendations.</u> <p>Post Office Limited are aware of this issue with the Foundstone Server and have decided not to make any changes or perform a refresh.</p> <p>Also see the follow-up action (above) for A9331408 which helps to address the issue of software and hardware support being withdrawn.</p>				
<u>Action:</u> <p>No further action to be taken.</p>				
A7709793	When the Fujitsu Debit Card Service (DEA) servers rehome, or if the network has an		X 25 is old technology, the nature of the failure is not applicable to other network services. No further tests could be	Yes

**FUJITSU RESTRICTED**

	issue, there appears to be an approximate 45 minute delay in the network connectivity being established with the Merchant Acquirer (GlobalPay).		done.	
<u>Findings and Recommendations.</u> X25 is old technology, the nature of the failure is not applicable to other network services. It is recommended that POL move this service away from the X25 technology.				
<u>Action:</u> No further action by POA is recommended.				
A7224474	At 10:55 on the 5th January the POLSAP Support team were made aware of an issue with POLSAP, whereby some users were experiencing slow performance and access issues. At 11:20 the POLSAP system hung in an indeterminate state. Problem Description POLSAP users were unable to log on to POLSAP between 11:20 and 12:09.	Further analysis into root cause is ongoing, however the investigation will be restricted, due to the file system having been rebuild.	It is considered that no further actions can take place.	Yes
<u>Findings and Recommendations.</u> The POLSAP team have reported that daily checks have been put in place at 08.00 hours before the system starts.				
<u>Action:</u> No further action is required as corrective action has been put in place.				
A7941790	Disruption to Network Banking Services on Sunday 15th March 2015 following the implementation of MSC 043J0427418-10, IRE11 Firewall Service Module	The underlying cause of the failure cannot be undertaken until the IOS operating system upgrade is implemented again. As this would induce a repeat failure	Give consideration to any further testing which can be performed on IOS upgrades before they are rolled out to the live estate.	Yes

**FUJITSU RESTRICTED**

	IOS update.	CISCO have recommended the Firewall IOS operating system remains at the current version until the Firewall hardware is upgraded. Post Office Limited are required to submit a change request to imitate a Firewall hardware upgrade.		
<u>Findings and Recommendations.</u> The CISCO Firewalls are being replaced as part of the HNG-X Data-Centre Refresh. This is expected to take place in Q2 2016 (April-June).				
<u>Action:</u> No further action is required as corrective action has been put in place.				
Administration Closures				
A10519660	Low Optical Power fault on DWDM link at FS-SDC02/1-MX03	This Problem Record was raised in error.	Admin Closure – No action.	Yes
A10364554	Can't connect to the Balfour Beatty tape library in SDC01	This Problem Record was raised in error.	Admin Closure – No action.	Yes
A10091154	Test Call	This was a test Problem Record.	Admin Closure – No action.	Yes
A7709307	Potential Delays in resolving incidents across the End to End Horizon Service.	This was a duplicate Problem Record – see A7503925 below.	Duplicate Problem Record Admin Closure - No action.	Yes
Issue in Third Party Domain				
A10519956	CGI have confirmed the Credence application is unavailable for all users	The underlying cause of this issue is that the G drive in Credence server had become full.	Issue in Third Party domain - No action.	Yes
A10443897	Manual Log On	The underlying cause of the	Issue in Third Party	Yes

**FUJITSU RESTRICTED**

	Credentials to Access First Rate sever	incident was that incorrect authentication details were incorrectly enter due to human error and that, as Secure File Transfer Protocol does not allow a manual break out, it is not possible to take corrective action, e.g., enter the correct authentication details	domain - No action	
A9401004	POA HNG-X are receiving unauthorised web service requests from POL Clients through to the Collect & Return (CWS) service via the Royal Mail portal.	On Friday 22 nd April 2016 a cross domain conf call was held with ATOS, POL, RMG and FJ. RMG advised us that they do undertake CustomerID checks on requests made to them and RMG have throttling on the number of requests they can be pass through to the CWS servers.	Issue in Third Party domain - No action.	Yes
A9130208	CSC implemented server changes within their environment which lead to Production POLSAP operational issues.	The issue in this Problem Record is also covered by A9129261 and A915777	Issue in Third Party domain - No action	Yes
A9129261	Unannounced and uncoordinated infrastructure changes are being implemented in third party domains which have caused serious service outages.	ATOS have moved this to Continual Service Improvement and are now managing this under CSI3893	Issue in Third Party domain - No action	Yes
A9101997	Since the 28th May 2015 Fujitsu Services have been unable to pull the E-Pay Daily Transaction Feed files.	This is reported as coinciding with a firewall change taking place within the third party domain. In any case the solution was to remove an unnecessary NAT rule in the E-pay -> Post Office direction and this change has been performed on both sites firewalls. The NAT rule that has been	Issue in Third Party domain - No action	Yes

**FUJITSU RESTRICTED**

		removed is unnecessary as connections are always made in the Post Office -> E-pay direction."		
A9042829	Monitoring is Alerting Radius Authentication Failure User-Name for the Branch Router at FAD 180523.	It is reported the branch closed in November 2014. ATOS/POL advise the router has now been removed from site.	Issue in Third Party domain - No action	Yes
A9040664	Monitoring is alerting mismatches between BAL and PIN Pad serial numbers.	The Problem Record was closed by ATOS. POL is to raise a Change Request on ComputaCenter to address this.	Issue in Third Party domain - No action	Yes
A8688801	Due to a faulty POL AP-ADC Script First Rate Branch Order Files are failing Transformation.	The fix was implemented in live on the 1st of June and no further failures in First Rate have been identified.	Issue in Third Party domain - No action	Yes
A7938892	Data from January and February 2015 shows monitoring events triggered by loss of connectivity to the Branch routers for AEI devices	This problem is within the AEI external domain	Issue in Third Party domain - No action	Yes
A7503925	Potential Delays in resolving incidents across the End to End Horizon Service.	FJ investigations have identified a possible SSL certificate issue within the 3rd Party domain. ATOS have moved this to Continual Service Improvement and are now managing this under CSI3821	Issue in Third Party domain - No action	Yes
A7503916	Incorrect Support Route Being Used – Non-conforming with agreed processes.	This problem is within the external domain	Issue in Third Party domain - No action	Yes
A7424176	The current route for the Ingenico Paystation file into Fujitsu is not	Improvement planned to send the file directly using SFTP so that the usual ITR error reporting/retry process would	Issue in Third Party domain - No action	Yes

**FUJITSU RESTRICTED**

	clearly understood by the Technical Support teams.	be used, this is part of the CIF519 POL Win in Mails development work		
A7332347	System Alerts are being raised for National Express Ticket services due to National Express stop lengths being greater than 50 characters for "ArrivalLocationStopName" and "DepartureLocationStopName".	This problem is within the external domain	Issue in Third Party domain - No action	Yes