FUJ00120476

POLSAP Hosting Service: Joint Working Document (Operational Level Agreement)

COMMERCIAL IN CONFIDENCE

Document Title:	POLSAP Hosting Service: Joint Working Document (Operational Level Agreement)
Document Type:	Operational Level Agreement (OLA)
Release:	POLSAP
Abstract:	Joint Working Document / Operational Level Agreement to support the: POLSAP Hosting Service provided to Post Office by Fujitsu Services.
Document Status:	APPROVED
Author & Dept:	David Nicholson Fujitsu Services
Internal Distribution:	Royal Mail Group Document Management & Reviewers
External Distribution:	Post Office Limited
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
James Davidson	Fujitsu Services, Director of Service Operations, Royal Mail Group Business Unit		
Tony Atkinson	Head of Service Operations, Royal Mail Group Business Unit		
Mark Weaver	Post Office Limited		

Note: See Royal Mail Group Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

FUJ00120476

0 Document Control

0.1 Table of Contents

FUJ00120476

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	01/07/10	New JWD to replace CS/SER/022. First draft for formal review.	
0.2	14/07/10	Changes requested by POL	
0.3	04/08/10	Changes requested by CSC	
0.4	26/08/10	Changes requested by POL after review	
0.5	07/09/10	Changes made to track all changes, before being issued for review	
0.6	13/09/10	Changes made to include all comments received before being issued for approval, and document amended to become a Service Description & a CCD	
0.7	07/10/10	Updated to include the Severity ratings.	
1.0	07/10/10	Issued for approval	
2.0	04/11/2010	Reference number changed from SVM/SDM/SD/0872 and title changed from **POLSAP Hosting Service: Joint Working Document**.	

FUJ00120476

0.3 Review Details

Review Comments by :	
Review Comments to :	david.nicholson@ GRO & PostOfficeAccountDocumentManagement@ GRO
Mandatory Review	
Role	Name
FJ CS Head of Service Operations	Tony Atkinson
FJ SI Programme Manager	Alistair Bach (*)
FJ Core Services Unix Operations Manager	Adrianne Thompson (*)
FJ Core Services Network Operations Manager	Ian Mills
FJ Core Services SMC Manager	Saheed Salawu (*)
FJ SAP Practice	Lynette Licence (*)
FJ Commercial Director	Guy Wilkerson
Post office Ltd, Commercial Director	Liz Tuddenham
Optional Review	
Role	Name
FJ CS Security & Risk Manager	Bill Membery (*)
FJ CS POLFS service Manager	Mike Stewart
FJ CS Business Continuity Manager	Adam Parker
FJ CS SSC Manager	Steve Parker
FJ SAP Practice	Eveline Bunce (*)
FJ CS Data centre and Infrastructure	Claire Drake
FJ SI Infrastructure Design	Pat Lywood
FJ Testing Manager	Debbie Richardson
FJ Operational Security	Donna Munro
FJ Data Centre Migration	Vince Cochrane
FJ Integration Team Manager	Vijesh Pandya
Post Office Ltd, Service Mgr	Dave Hulbert
Post Office Ltd, POL FS Project Manager	Glyn Drabble (*)
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
Post Office Ltd, Project Manager	Glyn Drabble
Post Office Ltd, Business Manager	Sean Farrow
Post Office Ltd, Service Delivery	David Wright (*)

0.4 Associated Documents (Internal & External)

FUJ00120476

	Reference	Version	Date	Title	Source
1	PGM/DCM/TEM/0001 (DO NOT REMOVE)	1.0	13/06/06	Fujitsu Services Royal Mail Group Account HNG-X Document Template	Dimensions
2	EA/IFS/001	3.0	17/06/04	HORIZON to POL –Finance Systems Interface Specification	PRISM
3	BP/DES/030			SAPADS to POL-FS Application Interface Specification	PRISM
5	SVM/SDM/OLA/0011			Operational Level Agreement for SAP Hosting Service	Fujitsu
6	SVM/SDM/PRO/0761			HNG-X Release Management Process	Fujitsu
7	SVM/SDM/SD/0003			Data Centre Operations Service: Service Description	Fujitsu
8	POLSAP/ARC/SVS/ARC/0001			Polsap Service Architecture	Fujitsu
9	POLSAP/DES/INF/HLD/0003			POLSAP High Level Design	Fujitsu
10	SVM/SDM/SD/0004			Third line support service description	Fujitsu
11	SVM/SDM/SD/0005			Forth line support service description	Fujitsu
12	SVM/SDM/SD/0007			Service Management Service: Service Description	Fujitsu
13	SVM/SDM/OLA/0015			Operational Level Agreement for Core division WINTEL & NT Near shore	Fujitsu
14	SVM/SDM/OLA/0018			Operational Level Agreement for the System Management Centre Service	Fujitsu
15	RS/POL/003			Horizon Access Control Policy	Fujitsu
16	SVM/SDM/PRO/0025			RMG BU Customer Service Problem Management Process	Fujitsu
17	POLSAP/SVM/SDM/SD/0873			POLSAP INCIDENT MANAGEMENT SERVICE DESCRIPTION	Fujitsu
18	POLSAP/SVM/SDM/OLA/0874			Operational Level Agreement for POLSAP Application Support Services	Fujitsu
19	SVM/SDM/PRO/0001			Major Incident Process	Fujitsu
20	SVM/SEC/STD/0750			Security Governance Guidelines	Fujitsu

Unless a specific version is referred to above, reference should be made to the current approved versions of the documents.

0.5 Abbreviations

Abbreviation	Definition
Agreement	The agreement between Post Office and Fujitsu Services dated 28 July 1999 (as amended, in particular by CCN 1100)
BAPI	Business Application Programming Interface (interface between 3rd party software and the SAP application)
COH	Cash on Hand

FUJ00120476

CIP	Cash in Pouches
CLE	Cash Centre Ledger Entry
Configured POL FS	The POL FS application that is configured by PRISM from SAP, to meet the business needs of Post Office. It includes all instances whether in live use, development or test.
Development SAP System	The platform used to host the SAP Software instance known as PLD, including PLD itself.
Fujitsu	Fujitsu Services Ltd
IDoc	Intermediate Document (is an SAP format for transferring the data for a business transaction
MSC	Managed Service Change
RMGA CS	Fujitsu Services Royal Mail Group Account Customer Services
RMGA SI	Fujitsu Services Royal Mail Group Account Systems Integration
POC	Pouch Collection
POD	Pouch Delivery
POL	Post Office Ltd
POL FS	Post Office Ltd Financial System
POL FS System	The technical infrastructure (forming part of the Horizon Service Infrastructure) employed by Fujitsu in providing the POL FS Services including, without limitation, the SAP System, and the communication links to, and equipment provided by Fujitsu at, Post Office Premises, to facilitate access by POL FS Users to Configured POL FS.
POSD	Post Office Service Desk
Post Office	Post Office Ltd
PRISM	An alliance of BT, CSC and Xansa, sub-contracting to Post Office Ltd for the configuration of Configured POL FS
Production SAP System	The platform used to host the SAP Software instance known as PLP, including PLP itself.
QA	Quality assurance
QA/Test SAP System	The platform used to host the SAP Software instances known as PLQ, PLN, and PLE, including PLQ, PLN, and PLE themselves.
SAP	A software based industry accounting system
SAP Basis	A software application providing a framework for the operation of the SAP System
SAP Front End	The software apparent to and used by POL FS Users to access Configured POL FS. It is also known as SAP Presentation Layer.
SAP Loading Applications	SAP software, configured by PRISM, for use by Fujitsu in loading data from Horizon and SAPADS onto Configured POL FS.
SAP System	The QA/Test SAP System, the Development SAP System and the Production SAP System
SAP ADS	The SAP Advanced Distribution System
SMC	Fujitsu Services Service Management Centre for dealing with issues raised by POL FS Users with the PRISM helpdesk where such issues relate to the POL FS System but the cause of them is not within Configured POL FS.
TfS	Triole for Service, the Fujitsu Call Management service
TMS	Transaction Management Service

0.6 Glossary

Term	Definition

FUJ00120476

0.7 Changes Expected

Changes
Issue V1,0, under revised doc ref of SVM/SDM/SD/0872

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.

FUJ00120476

1 Service Summary

Post Office operates two large SAP systems in separate data centres as separate instances, plus several legacy systems in Cash Centres. The POLSAP Service provides a consolidated SAP environment on a new blade frame infrastructure in the Fujitsu Post Office Ireland Data Centres to support business critical processes.

The following summarises each of the systems with in the POLSAP service:

(Note POLSAP R1 includes POLFS, SAPADS and CMS only)

POLFS

- A SAP 4.7 IS Retail System
- Implemented in 2004 (as part of the Impact Programme)
- Currently hosted by Fujitsu in Bootle and Wigan, with application support by CSC/Steria and SAP Basis support by Fujitsu
- Supports the financial settlement of transactions undertaken at the Post Office counters and via direct sales channels.
- 400 Users

SAPADS

- A SAP 4.6c application
- Implemented in 1997; currently hosted and supported by CSC/Steria
- Supports Supply Chain functions (mainly the warehousing and movement of cash through the Post Office network and to external customers)
- A customised application (upgrades are complex, protracted and costly)
- 825 Users

Transtrack

- 26 instances of Transtrack within the estate
- Used in Cash and Value in Transit depots (CViT) to track and trace inward and outward pouches
- 1400 users

CMS (Siebel)

- Holds details of the master contract data for all external customers serviced by CViT depots.
- c.25 users

CASHMAN

- Stand-alone Microsoft Access application
- Manages the inventory of cash and cassettes at ATMs
- Used in 5 Cash Centres
- c. 25 users

FUJ00120476

BUDMAN

- Stand-alone Microsoft Access application
- Manages the inventory of notes and coins owned by RBS and NatWest that are held in Post Office Ltd Cash Centres
- c. 10 users

FUJ00120476

2 POLSAP

2.1 POLSAP System

POLSAP will follow the same landscape model as POL-FS, with four tiers:

1. IRE11 – Production (PLP)
2. IRE19 – Development (PLD)
3. IRE19 – Two QAS/Test environments
   PLQ for technical integration testing
   PLE for Post Office testing and sign-off

Any new POLSAP functionality will be unit tested in Development, then migrated to PLQ for integration testing and on to PLE for User Acceptance testing. After sign-off the functionality will be migrated to production.

Post Office acceptance test users will access the PLE environment from the Royal Mail SAP Enterprise portal.

Please see the POL SAP System Landscape Overview document (FS/ERP/SSL/0001) for the rationale behind the four tier landscape and the SAP Practice Operational Level Agreement (see POLSAP/SVM/SDM/OLA/0874).

The majority of work to put in place the infrastructure and technical services required to host POLSAP will be achieved through deployment of the Horizon Online service in the Ireland Data Centres by the HNG-x programme, together with the migration of the POL-FS system from its current hosting environment in Bootle and Wigan.

The design for the migrated POL-FS solution is described in a separate High Level Design document (POLSAP/DES/INF/HLD/0001).

Figure 1 shows a high level view of the POLSAP Infrastructure and Infrastructure Services at the implementation of Phase 1.

The production system is hosted in the IRE11 data centre. Development and QAS/Test are hosted in IRE19, with that environment providing a production failover capability for POLSAP as part of the HNG-x Disaster Recovery model.

The migration steps that lead up to the convergence of POL-FS and SAPADS on a single platform are described in a separate POLSAP Migration High Level Design (POLSAP/DES/MIG/HLD/0001).

Fujitsu are responsible for all POLSAP application and SAP Basis support for POLSAP.

FUJ00120476

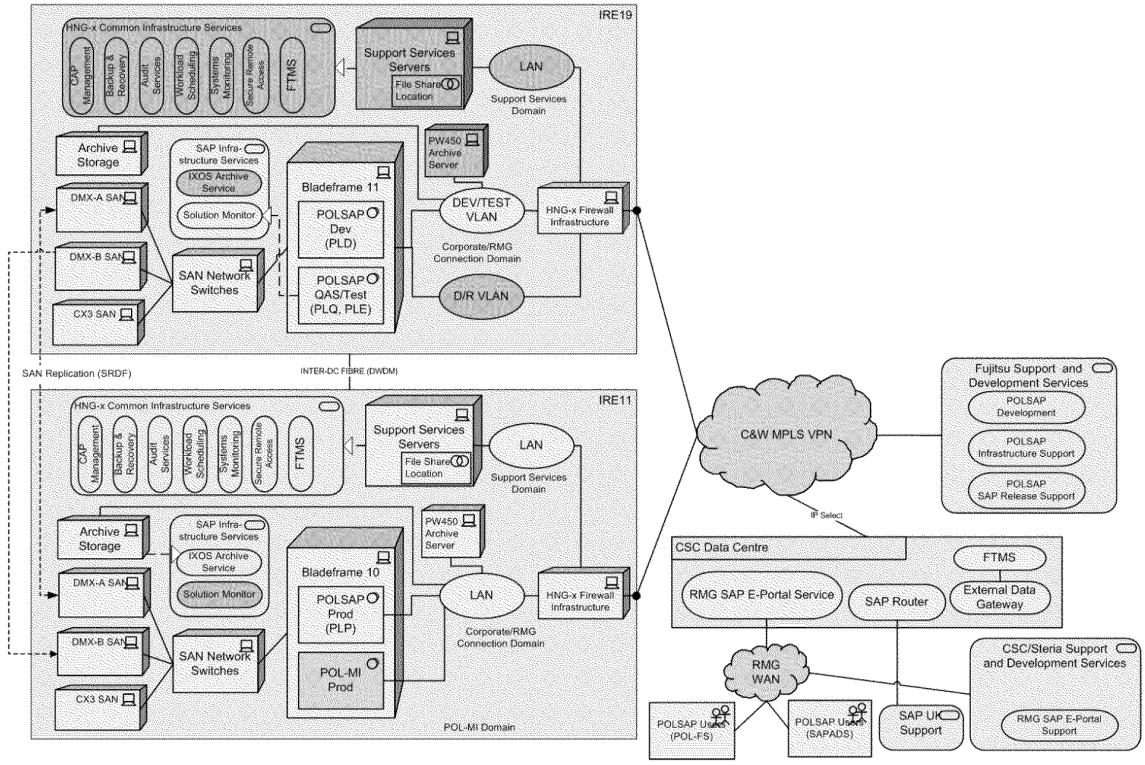

Figure 1 – POLSAP Technical Landscape

2.1.1 Version of SAP

POLSAP is based on SAP R3 IS Retail 4.7 extension set 110.

The R3 application consists of the SAP Database (also known as the SAP Host) that is at the core of the business application and a number of Application Servers that take processing load away from the SAP Host.

The Database Server controls all the majority of the SAP R3 processing activity and where batch jobs are to be processed they are triggered (by Tivoli Workload Scheduler) on the Database Server, all other jobs are triggered through Business Connector.

2.1.2 Other SAP Elements

SAP XI

SAP XI (Exchange Infrastructure) is SAP's enterprise application integration software and facilitates the exchange of information between the SAP application and external end points. XI supports a range of connectivity methods, data formats, and communication protocols.

FUJ00120476

For POLSAP, SAP XI is a requirement to support processing of key POL-FS interfaces including the Branch Ledger Entry data from HNG-x.

In a Disaster Recovery situation SAP XI services will continue to be required at the failover site.

SAP XI will also be used to process certain SAPADS interfaces as they are converged into POLSAP.

SAP Business Connector (BC)

SAP Business Connector is a legacy mechanism (integration server) that sits outside SAP R3 and uses a SAP adapter for BAPI and IDoc communication and processing.

For POLSAP R 1, the solution will have the capability of supporting SAP Business Connector interfaces. The SAPADS system currently uses Business Connector for interfacing to Transtrack and the large Note Counting machines.

In a Disaster Recovery situation SAP BC services will continue to be required at the failover site.

SAP Solution Monitor

SAP Solution Manager is used to manage the complete POLSAP SAP environment (Production, Development, QAS Test) for technical support and monitoring.

In a Disaster Recovery situation the SAP Solution Manager service will continue to be required at the failover site.

SAP Archiving Solution

The long term POLSAP archiving requirements have been documented within the POLSAP Archiving Strategy Document (FS/ERP/SAS/0001).

Please see the SAP Practice POLSAP OLA POLSAP/SVM/SDM/OLA/0874 for further details)

FUJ00120476

3 Service Definition

3.1 POL and FJS Division of responsibilities

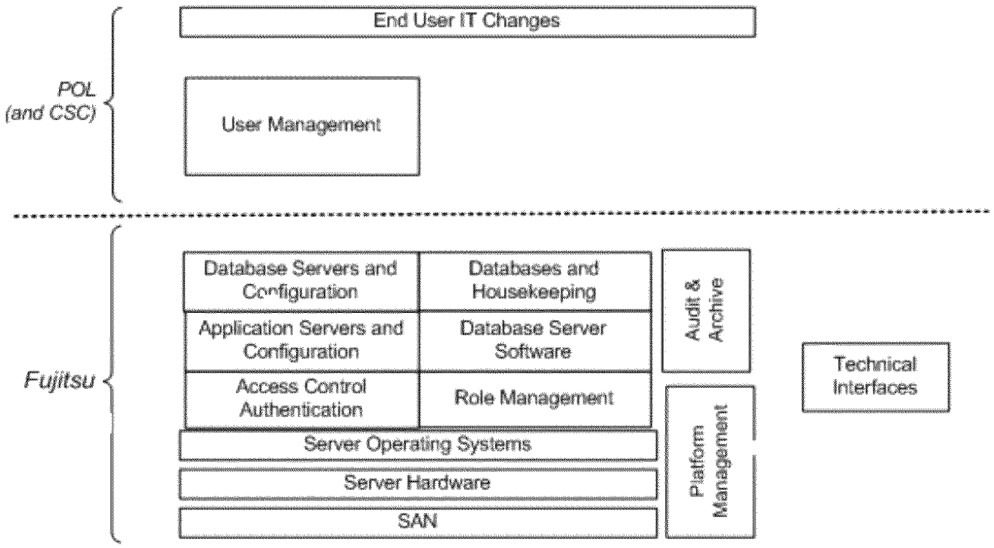

Figure 2 POLSAP Responsibilities

The end users access to POLSAP is via the Royal Mail SAP E-Portal, which is part of the CSC environment.

Fujitsu will however do the role management changes for POL as and when required. This has been projected to be less than 5 requests per month.

FUJ00120476

3.2 Key Fujitsu Service Responsibilities

Service Tower	Support Group	Location (Primary)	Location (Secondary)	Key Responsibility
System Management	SMC	Systems Management centre in India [24x7 Systems and Event Monitoring]		2nd line support to POLSAP service desk (1ST Line support to POLSAP users is being provided by CSC) and Incident mgmt. TfS interface to support groups. Manual interface to FMS for hardware break/fix.
Applications Mgmt and Support	Fujitsu SAP			3rd and 4th line support.
Datacentre Hosting	Fujitsu Data centres	IRE 11 Data Centre in Northern Ireland	IRE 19 Data Centre in Northern Ireland	DC Operations
Server and Storage Mgmt	Fujitsu ISD Operations	IRE 11/19 Data Centres in Northern Ireland	n/a	Server and Storage Operations
Network Mgmt	Fujitsu IS			LAN/WAN/Firewalls- 2nd & 3rd line incident support, plus change and release deployment

3.3 Service Elements

3.3.1 In scope for Fujitsu

The following elements are in scope for Fujitsu in the provision of the POLSAP service

- SAP Application development – any changes which are deemed of a significant size and or scope or change of functionality will need to be subject to CR.
- Application interfaces development
- Functional testing
- Data Centre hosting
- Disaster Recovery
- Tiered SAP Environments to support live operation, development, and quality assurance testing
- SAP XI
- Platforms for Application Servers, Database Servers, SAP Solution Manager, Archiving
- Storage for Business Data and to support platform and service operation
- Systems Management for the hosted solution
- Hardware Break/fix for platforms and Data Centre network
- Operating System and Database Management for the hosted solution

FUJ00120476

- Service Management
- System Management (SMC Only), Incident Management, Problem Management, Change Management, Configuration Management, Release Management, Security Management.
- Ongoing Application Support, including SAP Basis and SAP XI Administration, Interfaces support
- Enabling end-user access via a resilient network connection to the Royal Mail network. (This link will support Post Office on-line user access from the Royal Mail SAP Enterprise Portal).
- Enabling data exchange to end-point systems on the Royal Mail network
- Enabling data exchange to external end-point systems
- User Role Maintenance
- Total POL (indicative) user base of …
    - POL FS 400 users
    - SAPADS 825 users
    - TransTrack, Budman, and Cashman 1435 users
    - CMS/Siebel 25 users
    - SAP-XI 25 users

3.3.2 Not in Scope for Fujitsu

The following elements are NOT in scope for Fujitsu in the provision of the POLSAP service

- End user IT (desktops, laptops, printers etc.)
- Provision and support of the Royal Mail SAP Enterprise Portal. The portal is provided by CSC/Steria and is a dependency that POLSAP users have for successfully accessing the POLSAP service.
- Environments for Post Office's development, other than the shared development environment
- Any infrastructure specifically for integration with any mobile device including the sending of SMS text messages.
- SAP Internet Transaction Server (ITS). CSC are responsible for provision of the ITS service. Fujitsu will need to work closely with CSC to ensure that ITS is properly integrated to the POLSAP service
- POLSAP SAP licence management and maintenance. POL is responsible for SAP licence provision to Fujitsu to provide support for the POLSAP service.

3.3.3 In scope for CSC

The following elements are in scope for CSC in the provision of the POLSAP service

- Log and Management of calls
- Log calls, from RMG employees, and create an incident on Remedy SRT against the specified application. Call logging will be carried out 24*7.
- Pass the call details to Fujitsu by logging an incident on the Triole system - 24*7
- Contact Fujitsu Service Desk via phone in the event of a sev1 or sev 2 incident being identified

FUJ00120476

- Provide RMG with updates by using the Triole system to provide the most up to date information. Chase calls to Fujitsu will only be made within core hours of 8-6 Monday to Friday unless a sev1 or 2 incident.
- CSC to update the SRT record with information provided to them by Fujitsu and with any updates provided to Fujitsu. There is no automated interface between TfS and Remedy.
- Fujitsu to contact CSC helpdesk via E-mail / telephone or Triole to confirm call can be closed.
- CSC to update and close the call.
- CSC to interface between several 3rd parties as necessary
- CSC to inform Fujitsu of any CSC incidents that will impact Fujitsu either by email or other specified mechanism and update SRT ticket accordingly
- Managing Helpdesk knowledge scripts and incorporating agreed changes to knowledge scripts

3.3.4 Not in Scope for CSC

The following elements are NOT in scope for CSC in the provision of the POLSAP service

- Confirmation of call resolution with end user
- Major Incident management
- Problem Management
- Change Management
- SLA Management
- SLA Reporting
- Customer Satisfaction Survey
- Reporting

3.4 POLSAP Platform Hosting

- Fujitsu hosts the Development POLSAP System and Production SAP System within its Data Centres in Ireland (IRE11 and IRE19)
- The QA/Test SAP System acts as the fail-over system for the Production POLSAP System. There is no fail-over system for the Development or QA/Test systems. The time taken for failover and the QA/Test POLSAP System being re-configured for use as the Production POLSAP System will take approximately 48 hours.
- In the event that we failover to the QA/Test system, there is no further resilience for the DR Production Service.
- Fujitsu has extended its standard Datacentre hardware and operating system maintenance and administration functions to encompass the POLSAP System. These are detailed within the Data Centre Operations Service Description (SVM/SDM/SD/0003)
- Fujitsu will at all times maintain the integrity of data within the POLSAP System.
- The access control policy set will be applicable in relation to the SAP System. In addition:

FUJ00120476

- Fujitsu will take reasonable steps to protect the SAP System from unauthorised external intrusion; and
- Access to individual SAP Software instances as described in Section 2.2 will be restricted to authorised users.
- Fujitsu will manage and operate the technical interfaces for POL SAP.
- POLSAP will be managed through the HNG-x common infrastructure services for Systems Management (SYSMAN3/Tivoli) and Backup/Recovery, supplemented by SAP-specific systems management tools.
- Tivoli Workload Scheduler (TWS) will manage and run the majority of POLSAP batch processing and backup schedules. All others are triggered through the Business Connector.
- Scheduled Weekly full backups will be taken by Belfast Operations of all platforms. For the volatile business data a full backup will be taken weekly using RMAN software, with cumulative incremental daily backups in between.
- All data that is backed up will be held on SAN Tier C (CLARiiON) Storage. Backup images are replicated between data centres using a step in the workload schedule. This gives a resilient solution to backup that effectively has built in 'off-site' storage without taking tape backups or utilising a non Data Centre location for tape storage. The two most recent copies of the weekly full backup are retained for safety,
- The POLSAP Oracle database has been initially sized for 5Tb.

3.5 Network Connectivity (WAN)

POLSAP has capability of being supported remotely by Fujitsu Infrastructure and Application teams. All Fujitsu support teams will be connected to the Fujitsu corporate network.

Online end user access to production POLSAP is primarily through the CSC/Steria managed presentation:

- The majority of on-line users access POLSAP via CSC/Steria hosted and managed SAP E-Portals.
- There are a number of on-line users who access a Citrix server, hosted and managed by CSC, and then use SAPGUI to access POLSAP

All printing will be by one of two routes:

- Reports directed from POLSAP to a CSC hosted/managed File/Print Service, then on to specific printers
- Browser-based display of reports by end-users, sent by users for printing on local CSC managed printers

(Note Printing is not the responsibility of Fujitsu)

The majority of file transfer activity between POLSAP and Royal Mail systems will take place using the File Transfer Management Service (FTMS). This is an existing service.

Fujitsu manages the WAN links to Ireland Data Centres, through the provision and support of required Network circuits, routers, switches, firewalls and other associated hardware.

The solution is hosted within the HNG-x Corporate/RMG Connection Domain

The POLSAP solution maintains the range of interfaces currently supporting the POL-FS and SAPADS services, supporting:

FUJ00120476

- The required protocols and interface mechanisms
- The equivalent integrity and security monitoring associated with the interfaces
- levels of processing efficiency

The interfaces for POLSAP are documented in the POLSAP Blueprint Document (FS/SG/SBP/0001), taken from the Blueprint document summarises the interfaces deployed at POLSAP R1. Also see EA/IFS/030 v6.6: Technical Interface Specification Impact Programme: POLFS S80 Technical Interface Specifications

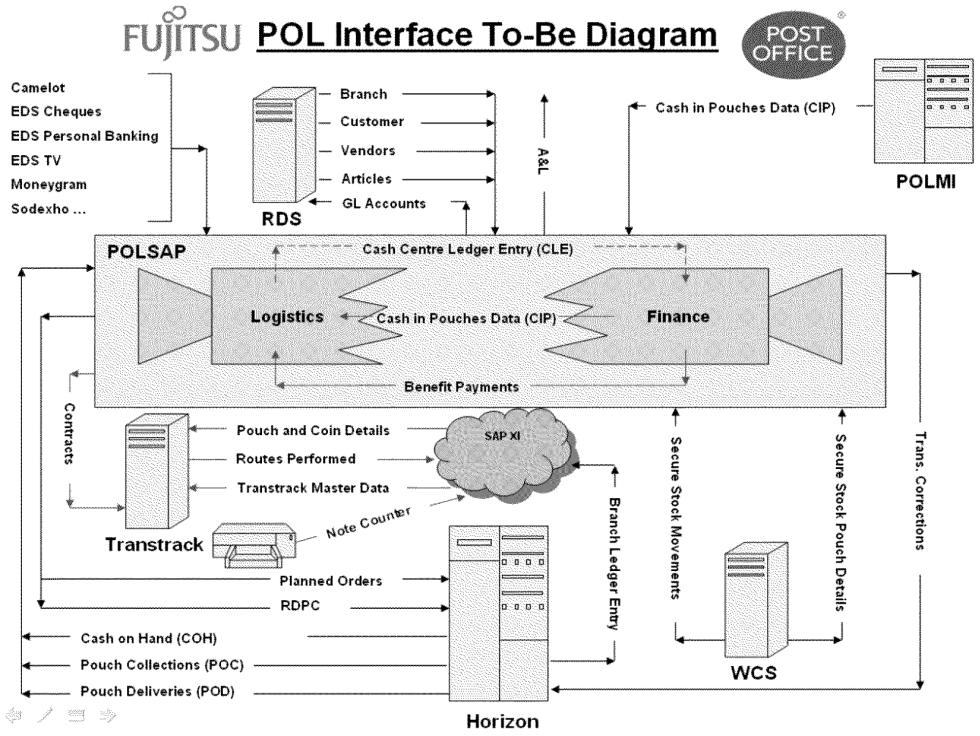

Figure 3 – POLSAP Interface To-Be Diagram

POLSAP utilises the HNG-x data centre networking infrastructure and introduces no new network components.

POLSAP is hosted in the HNG-x 'Corporate / RMG Access" security domain, and will comply with all security policies associated with systems deployed in that domain.

A network Low level Design has been produced for POLSAP (POLSAP/DEV/INF/LLD/0121).

3.6 POLSAP Application Management

- Fujitsu will via Fourth Line Support SAP practice:

  a) manage daily administration and system monitoring functions of POLSAP;

FUJ00120476

b) monitor the performance of POLSAP; and

c) undertake performance management of POLSAP Basis on a daily basis.

(See SVM/SDM/SD0005 Forth line support service description)

- The Fujitsu Fourth Line support SAP Practice combines both UK and Offshore (India) resource

3.6.1 Managing the POLSAP Instances

SAP Solution Manager will manage the Production, Development, and QAS/Test environments.

SAP Solution Manager will be deployed for the monitoring and administration of the SAP landscape.

SAP Solution Manager will co-reside on a SAP XI Database pBlade and will monitor all SAP instances, i.e. Solution Manager in IRE19 will monitor SAP Instances in IRE11 and IRE19.

The deployment model for Solution Manager is depicted at Figure 4 taken from the POLSAP High Level Design

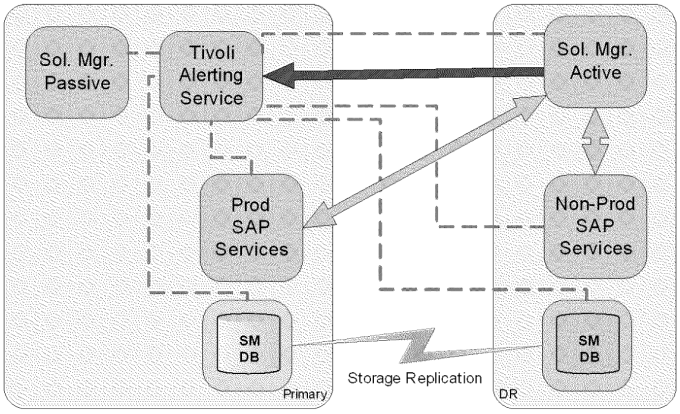

Figure 4 - Solution Manager Deployment Model

On-line access to the SAP Solution Manager GUI will be via authenticated connection to the HNG-X Secure Access Server (SAS) service (Platform code: SSN).

SAP Solution Manager will be installed on one of the XI Database Blade Servers in IRE19 (with a standby copy in IRE11).

3.6.2 Remote Access

To allow approved Fujitsu staff to gain administrative access to system consoles, Fujitsu uses “Secure Access Servers (SSN)”. SAPGUI will be deployed to the SSN Servers.

Support users provide two forms of authentication to log on to the Secure Access Servers with Windows Terminal Server client software loaded onto their PCs. Once they are logged on, they have access to a pre-defined set of administrative tools, each of which has access through the firewall to a pre-defined set of managed systems.

FUJ00120476

The standard set of management tools includes the SSH client, which allows recorded, command-line access to any managed host, via an X-Windows client.

FUJ00120476

4 Service Management

4.1 Service Management Scope

- Fujitsu has appointed a Service Delivery Manager for the POLSAP Services.
- The Service Delivery Manager responsibilities are defined in SVM/SDM/SD/0007 Service Management Service: Service Description and include:
    - monitoring service performance;
    - ensuring management of the resolution of any issues that arise; and
    - representing Fujitsu at the POLSAP service review forum

The following Services will apply in relation to the POLSAP System and are covered in Service Management:

System Management Centre

Incident and Problem Management

Change and Release Management

Configuration Management

Service Level Management

Capacity Management

Business Continuity and DR

Security Management

4.2 System Management Centre

Service Management Centre (SMC) will be the Fujitsu Services System Management operation, i.e. SMC based in India. For the Service Management Centre operational level agreement see SVM/SDM/OLA/0018.

Fujitsu has extended the existing FJS Service Management (SMC) to cover POLSAP Service. The agents at the Fujitsu Service centre will receive training on the POLSAP Solution and how it underpins Post Office® critical business processes, thus allowing them to empathise with callers, understand the business impact of issues and provide an enhanced user experience.

The SMC Service Centre uses Fujitsu's Service Management tool (TRIOLE for Services) which has been designed and implemented to be in line with ITIL processes and adhere to the ISO20000 standards.

SMC capability is available:

00:00 – 23:59, 7 days a week

The Service provides on all days of the year including all English Bank Holidays but excluding Christmas Day. The Service Centre will accept calls from CSC on behalf of Post Office Limited internal

FUJ00120476

departments, and Post Office Clients (and calls from internal Fujitsu Services capability and support units).

Post Office Limited Help Desk will provide 1st line Service Desk support functions to its end-user population (This service is provided by CSC (Call Logging). Fujitsu's SMC will provide 2nd line support and for 3rd line Incidents, these will be passed to Fujitsu support groups for action (e.g. incident/problem resolution or implementation).

The 1st line CSC service desk will be able to contact the FS Service Desk either by telephone or through the Triole service.

CSC should log a call on the Triole system and pass the call through the SMC stack (POLSAP SMC stack) who will then triage the call and pass it on to the relevant SDU.

All Severity 1 and 2 calls must be accompanied by a telephone call (i.e. warm handover) rather than just being passed over as these calls are more time sensitive and require an immediate response.

4.3 Incident and Problem Management

- Fujitsu is responsible for all POLSAP Application support.
- There will be a Fujitsu Services Duty Manager available for problem escalation 24 hours a day, 7 days a week.
- SMC support for scheduled batch activity will be available overnight, as well as during the working day.
- For the Systems Management Service Description see SVM/SDM/SD/0006.

Incidents may arise relating to the POLSAP. Post Office will be responsible for ensuring that all incidents reported by POLSAP Users are initially reported by telephone to the CSC helpdesk.

Incident management for POLSAP will be managed in accordance with the Incident Management process as described in POLSAP/SVM/.SDM/SD/0873.

The CSC service desk will log the incident on their call management system and carryout an initial investigation on the incident root cause/resolution. If the incident is deemed to be within the responsibilities of POL/CSC as defined in this document then they will manage that incident to closure.

Where the cause of such an incident is within POLSAP under the responsibilities of Fujitsu, the CSC helpdesk will log the call in Triole and pass the call onto the POLSAP SMC stack. In doing so, the CSC helpdesk will continue to manage the interface with the POLSAP User; when a resolution or update for an incident is available, CSC will have visibility of the update and be able to pass that information to the POLSAP User.

The SMC may also pass calls to the CSC helpdesk stack, for example, where the fault is determined to be in the SAP Front End E Portal or where the fault is deemed to be outside the control of Fujitsu.

The SMC will route calls internally within Fujitsu as appropriate. Calls may be routed to:

a) the Fujitsu development or testing teams;

b) the Fujitsu POLSAP support team;

c) the Fujitsu hardware and operating system maintenance teams; or

d) the Fujitsu networking teams.

FUJ00120476

Calls may be logged by the CSC helpdesk with the SMC at any time. The SMC will be manned 24 hours a day, 7 days a week, and offers a single point of contact for passing calls from and to the CSC helpdesk.

Application support and support from system analysts required to resolve incidents will be available during normal business hours of 08:00 to 18:00 Monday to Friday, excluding English bank holidays.

Outside such normal business hours, engineering support (other than in relation to SAP Basis) will be provided in respect of calls categorised as 'A' and B priority and these will be escalated by the SMC to engineers providing cover on a call-out basis 24 hours a day, 7 days a week. Also have out of hours cover from 0600 – 0800 & 1800 – 2200 M-F and 0900 – 1700 Saturdays and bank holidays for application incidents in the MM/LIS/WM functionality for A and B priority incidents.

Major Incident Management for POLSAP will be managed in accordance with the Major Incident Management process as described in SVM/SDM/PRO/0001..

Problem Management for POLSAP will be managed in accordance with the problem management process (as described in SVM/SDM/PRO/0025). Fujitsu Service Management and POLSAP support teams will proactively perform investigations into the root cause of incidents. All known problem actions will be documented by the RMGA Service Support team and discussed at the monthly service review.

4.4 Change Management and Release Management

The Service Management Service is responsible for the Operational Change process to ensure urgent operational changes to the POLSAP Service Infrastructure are implemented in a timely, accurate, controlled and secure manner without any adverse effect on the availability of the POLSAP Services and POLSAP Service Infrastructure, unless otherwise agreed between the Parties. As part of the Operational Change process Fujitsu services may also raise a Managed Service Change (MSC) to facilitate the change within Fujitsu support groups.

The Service Management Service will ensure that:

(a) no changes will be carried out without an approved MSC unless the change is to resolve an Incident adversely affecting the POLSAP Services;

(b) changes relating to Incidents where the change has been implemented to resolve the Incident without an approved MSC should be documented with a retrospective MSC;

(c) changes will not be carried out that affect the ability of POLSAP to serve users during Post Office Core Day except by prior agreement with Post Office; and

(d) the change originator is responsible for ensuring that the change is completed in accordance with ITIL service management best practice. Appropriate levels of implementation, communication, regression and test planning must be completed.

The Operational Change process shall be carried out in the following manner:

(a) MSC's may be raised by Post Office via the submission of a Change Request or by Fujitsu Services.

(b) the MSC originator must clearly document:

- the reason for the change;
- the POLSAP Services or POLSAP Service Infrastructure platform requiring the implementation of the change;
- the timescale in which the approval and change should take place; and

FUJ00120476

- any known effect of the change on the provision of the POLSAP Services or POLSAP Service Infrastructure;

(c) MSCs will be entered into a central Service Management Service database and then distributed to the appropriate Operational Services, Fujitsu Services' suppliers and Post Office and where it has an impact or potential impact, to provide comments and authorisation for the implementation of the change;

(d) if any of the authorising parties challenge or disagree with the content of the MSC and therefore request withdrawal or deferral of the planned change, this will be managed by the Service Management Service and the MSC will be re-issued following amendment or the proposed change cancelled;

(e) where an MSC has been issued retrospectively, the MSC is distributed to the appropriate Operational Services, Fujitsu Services' suppliers and, if necessary, Post Office, for advice and audit purposes only. In such circumstances, no MSC approval is required;

(f) following the successful implementation of a change, the Service Management Service will ensure the appropriate Operational Service arranges for the documentation relating to procedure, process or design, to be updated to reflect the change.

4.5 Configuration Management

The Fujitsu Service Management Service is responsible for the administration, management and control of all configuration management activities, within the POLSAP Service Infrastructure.

The Fujitsu Service Management Service shall be responsible for maintenance and management of configuration management reports produced by Fujitsu and such reports shall be available to Post Office upon request.

4.6 Service Level Management

A joint operational review forum will be established by service managers from all parties, to consider the performance of the services against their targets.

Support for the Service should be available during the hours of service measurement i.e. 07:00-19:00 Mon-Fri (excl. English Bank Holidays). Any problems outside these hours will be handled by on-call staff.

The reporting schedule needs to be defined, but it is expected that this will fit in with existing Horizon reporting. However it may be necessary to have periodic reviews with Post Office present.

For the Service Management Service Description see SVM/SDM/SD/0007.

4.7 Charges

The charges for this Service are laid out in Schedule D1 of the Agreement.

There maybe be times when an Ad-Hoc service charge will be applicable for Operational Change/ Functional Change see below.

4.8 Capacity Management

Business level Capacity Management will continue in line with the current POL-FS solution, but will become more of a point of focus with the Capacity Management Service than POL-FS. Component level Capacity Management on POLSAP will use the HNG-X solution. Metron Athene will be used to

FUJ00120476

capture CPU, Memory, I/O (disk and network), Oracle and process level data on all systems. This data will then be collected by the HNG-X performance database and stored on it. Such data will then be regularly analysed by the HNG-X Capacity Management Service to make sure there is sufficient capacity, indicate any opportunities for consolidation, and will be crucial for diagnosis in the event of an issue. Automated reporting will highlight any issues and thresholds that have been breached. In addition to the standard data captured by Athene, various supplementary data will also be captured including for Network (NNM), Storage (EMC Performance Manager) and BladeFrame. As well as helping to understand the solution operation in more depth, this data will also be used to measure and manage capacity of shared components that the POLSAP uses. Forecasting will include usage and projected usage for the service.

4.9 Business Continuity and DR

- Fujitsu Services is responsible for maintaining business continuity arrangements for the Service Management Service and sharing this information with Post Office as requested.
- Fujitsu Services and Post Office Business Continuity Managers will agree a plan of action in accordance with the Major Business Continuity Incident Management Process (MBCI) as defined in the described in the Working Document entitled: *"Major Incident Process", (SVM/SDM/PRO/0001)*.

4.10 Security Management

Fujitsu Services are, as per the RMG Account Information Security Policy (SVM/SEC/POL/0003), responsible for implementing, managing and maintaining a security framework, based upon Post Office Limited contracted security requirements, and in compliance with ISO27001 (Information Security Management Standard)

In August 2010 the Fujitsu Services RMG Account were positively recommended, by the British Standards Institute, for formal registration to ISO27001. the scope being:

"The operation and maintenance of the Royal Mail Group Account (RMGA) on-shore and off-shore services provided by Fujitsu to Post Office Ltd (POL) and incorporating the Horizon on Line Service and POL Financial Systems (SAP and Management Information). In accordance with the Statement of Applicability Version 8"

As per document SVM/SEC/STD/0750 – Fujitsu will follow guidelines set out in this document to ensure it retains its BSI ISO27001 accreditation.

4.11 Service Availability & Contact Lists

The SAP Production Service will be available to be logged onto by POLSAP Users 24x7 except by agreement – section 6.1 of the Service Architecture document refers.

Maintenance Slots. Downtime needs to be agreed with the customer one week prior to the requested date.

There will be a Fujitsu Duty Manager available 24 hours a day, 7 days a week. The Fujitsu Duty Manager will be available as a point of contact for Post Office in the event that a problem requires escalation.

Fujitsu Services POLSAP Service Management Contacts

Monday – Friday, 08:30 to 18:00 only.

FUJ00120476

Prime Contact	David Nicholson	GRO
	GRO	
Escalation	Peter Thompson	GRO
	GRO	

Post Office POLSAP Service Management Contacts

Monday – Friday, 08:30 to 18:00 only.

Prime Contact:	Post Office Service Desk (24x7)	GRO
	GRO	
Escalation:	Ian Humphries	GRO

4.12 Operating System

Fujitsu Services will provide NT (Windows) & UNIX support for equipment hosted in the IRE11/19 Data Centres. This will be provided by on-site cover for 08:00 to 18:00 and by call out, outside of these daily hours.

Any Backups/ Maintenance work must be agreed prior to actioning via an MSC and can be planned for any Sunday AM, within the calendar year.

4.13 Supporting and Calculating Service Level Performance

The availability of the service and support is covered in the POLSAP service architecture document. ref POLSAPARCSVSARC0001

4.14 Service Dependencies and Assumptions

- CSC acts as a subcontractor to Post Office. As such, their responsibilities to deliver aspects of the SAP end-to-end service are not managed by Fujitsu and are not part of the service delivered by Fujitsu.
- There is no requirement for printing on special stationery so Fujitsu will provide no facilities for this.
- Products known as SAP ITS and e-Portal will be used by CSC/STERIA and POL for the SAP Front End.

FUJ00120476

5 Post Office Responsibilities

In addition to any other responsibilities of Post Office specified in this document and those responsibilities stated as not in scope for Fujitsu, Post Office will be responsible for:

- Provision of everything necessary for POLSAP users to access POLSAP beyond that provided by the Fujitsu Services and the POLSAP Service Infrastructure including, without limitation, configuration of the SAP Front End;
- Management of POLSAP Users and the definition and management of POLSAP User maintenance at the portal front end.
- Ensuring that POLSAP has the desired functional or business effect
- Approving changes to POLSAP through the authorisation of Operational Change Process via MSC's or SAP Transports.
- Training of new and existing POLSAP users on the POLSAP service.
- Providing detailed requirements of any changes required to this service due to legislative or standards which it is required to meet. In addition it will ensure that all appropriate rights of audit are available for Fujitsu to maintain its ISO 27001 accreditation. It will also ensure that all audits it requires are via a documented change control process with clear scopings and agreed payments with Fujitsu

FUJ00120476

6 Control Mechanisms

The contractual measures that apply to this service are described in the POLSAP Service Description (SVM/SDM/SD/0001)

This covers service availability (detailed below), service levels (detailed below), service definition, incident prioritisation, service targets and limits and HSD / SMC performance reporting.

In addition, internal measures may apply for specific productivity and service improvement activities.

6.1 SLA's

In order to ensure that the POLSAP service meets the business expectations, a suite of SLA's have been agreed. The SLA's listed below are purely those for the service provided by Fujitsu Services, dedicated to the POLSAP service.

SLA's for connectivity and desktop services provided by CSC are RMG wide services and, as such, are contained in RMG documentation.

- The service will guarantee the Availability SLA as detailed below:

AVAILABILITY ITEM	AVAIILABILITY PERCENTAGE PER MONTH	COMMENTS
Availability of Service with full redundancy	99.50%	The % of time POLSAP is available to be logged into by end-users, in comparison to total time during core service hours measured over a rolling month. Outages to be measured from time incident logged with Fujitsu Service Desk to successful resolution. This target excludes planned maintenance outage Availability will be measured between 06:00hrs and 22:00hrs Mon to Fri.

- The maximum downtime permitted during a single outage as detailed below:

MAXIMIUM OUTAGE	DOWNTIME PER MONTH	COMMENTS
Maximum Downtime permitted during a single outage	10 working Hours	The maximum unplanned outage time allowed on any single occasion where service is unavailable to end-users during core service hours Mon-Fri, measured over a fixed month. Outages to be measured from time incident logged with Fujitsu Service Desk to successful resolution.

FUJ00120476

- The Core Support hours are as follows:

SEVERITY	CORE SERVICE WINDOW	OUT OF HOURS SUPPORT	SERVICE RESTORATION	COMMENTS
Severity 1	Normal Working Hours: • Mon-Fri 08:00-18:00.	• Application Standby on Call for MM/LIS/WM Priority A and B incidents only. • Mon-Fri 06:00hrs to 08:00hrs and 18:00hrs to 22:00hrs • Sat - 09:00-17:00 • Public Holidays 09:00-17:00	-Initial response 20mins from SMC -Action Plan or Workaround within 2 working hours -Fix time 6 working hours -Additional 2 working hours if restoration requires a hardware engineer or replacement part - Incidents that have been identified as requiring support from SAP, or other 3rd Parties outside the control of Fujitsu, will be reviewed as part of the monthly service review and, if deemed to have breached SLA, will be subject to an agreement to remove them from the failure log statistics following the demonstration of all action taken by Fujitsu"	The following functions are considered Priority A and an incident should be raised as such in the event of an outage: • Critical • Business Stopped, Post Office unable to process any business or central system failure which will result in a number of Post Office/Departments being unable to process work • Complete loss of application • Outage of key infrastructure • Security Incident
Severity 2	Normal Working Hours: • Mon-Fri 08:00-18:00.	• Application Standby on Call for MM/LIS/WM Priority A and B incidents only.	-Initial Response within 1 working hour from SMC -Action Plan or workaround within 4 working hours -Fix time two working days	The following functions are considered Priority B and an incident should be raised as such in the event of an outage: • Major • Business

FUJ00120476

		• Mon-Fri 06:00hrs to 08:00hrs and 18:00hrs to 22:00hrs • Sat - 09:00-17:00 • Public Holidays 09:00-17:00		• restricted, a post office or department is restricted in its ability to transact business • Loss of key function of application
Severity 3	Normal Working Hours: • Mon-Fri 08:00-18:00	• Application Standby on Call for MM/LIS/WM Priority A and B incidents only. • Mon-Fri 06:00hrs to 08:00hrs and 18:00hrs to 22:00hrs • Sat - 09:00-17:00 • Public Holidays 09:00-17:00	-Initial response within one working day -Action Plan or workaround within three working days - fix time of six working days	The following functions are considered Priority C and an incident should be raised as such in the event of an outage: - Medium - Non critical, Post office working normally but with know disability e.g. work around provided. - Loss of non key function - Single user affecting incidents on key function causing business disruption
Severity 4	Normal Working Hours: • Mon-Fri 08:00-18:00	• Application Standby on Call for MM/LIS/WM Priority A and B incidents only. • Mon-Fri 06:00hrs to 08:00hrs and	-Initial response within 5 working days - Action plan or workaround within 15 working days - fix time of 28 working days	The following functions are considered Priority D and an incident should be raised as such in the event of an outage: - Low - Single-user affecting incidents on non key functionality

FUJ00120476

		• 18:00hrs to 22:00hrs • Sat - 09:00-17:00 • Public Holidays 09:00-17:00.		- Non disruptive multi users affecting incidents -Service requests - Non user affecting incidents.

- The Data Load Completion Metric is as follows:

DATA LOAD COMPLETION TIME	COMPLETION TIME	COMMENTS
Completion Time for Overnight Run of the batch schedule as agreed in *Datacentre Ops Service Description SVM/SDM/SD/0003 document.*	07:30	This Metric is as per the agreed batch schedule between Fujitsu Services and POL

- The Transaction Performance Metric is as follows:

TRANSACTION PERFORMANCE METRIC	VALUE	COMMENTS
Maximum Average time for each SAP transaction	1.5 Seconds	The maximum average time for each transaction in an agreed set of transaction types, measured over a fixed month. Time to be measured within the hosting environment and excluding WAN and presentation.

- The Disaster Recovery Target is as follows:

DISASTER RECOVERY TARGET	TIME	COMMENTS
Recovery of Service following a disaster	48 Hours	The maximum time for recovery to full service operation. Recovery will be to last known point of stability/data integrity, which is point (*tbc*) Recovery of service will be in accordance

FUJ00120476

		with the agreed ITSCM plan.