FUJ00232658

Document Title:	**HNG-X Support Services Business Continuity Plan**
Document Reference:	SVM/SDM/PLA/0001
Document Type:	Plan
Release:	Release Independent
Abstract:	This plan provides a summarised description of the HNG-X support service. This document also details the planned actions which can be taken to minimise the risk of one or more of these services not being available.
Document Status:	Approved
Author & Dept:	Changdev Pawashe, Business Continuity.
Internal Distribution:	Tony Atkinson, Steve Parker, Alex Kemp, Leighton Machin, Andy Hemingway, Andrew Gibson, Craig Rogers, Ed Ashford
External Distribution:	Anna Schofield, Disaster Recovery Analyst, Post Office Account, ATOS. APPROVED Versions only
Security Risk Assessment Confirmed	YES, security risks have been assessed, see section 0.9 for details.

UNCONTROLLED IF PRINTED

Name	Role	Signature	Date
Alex Kemp	Senior Operations Manager		

This Business Continuity plan is one of four. If the POA Duty Manager (or other authorised person) is unable to find the failed infrastructure service or components in this plan they are mandated to refer to SVM/SDM/PLA/0002 the HNG-X SERVICES BUSINESS CONTINUITY PLAN.

In the unlikely event of an HNG-X Security violation the POA Duty Manager (or other authorised person) is referred to SVM/SDM/PLA/0031 the HNG-X Security Business Continuity Plan.

A fourth Business Continuity plan SVM/SDM/PLA/0030 the HNG-X Engineering Business Continuity Plan has been produced to specifically cover the Engineering Service provided by Fujitsu Services Field Maintenance Services.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

0 Document Control

0.1 Table of Contents

0 DOCUMENT CONTROL 2

0.2 Document History 9
0.3 Review Details 10
0.5 Abbreviations 14
0.6 Glossary 19
0.7 Changes Expected 19
0.8 Accuracy 20
0.9 Security Risk Assessment 20

1.0 INTRODUCTION 21

1.1 Using this document 21
1.2 Business Continuity Plans for HNG-X 21

2 SCOPE 23

3 OWNERSHIP AND OPERATION 23

4 SERVICE FUNCTIONALITY 24

4.1 Services Overview 24
4.1.1 Infrastructure Sub-services 26
4.1.2 Operational Support Sub-Services 26
4.2 Infrastructure Support Services 26
4.2.1 The Security Management Service 27
4.2.1.1 Security Strategy 27
4.2.1.1.1 Application 28
4.2.1.1.2 Data 28
4.2.1.1.3 Operating System 28
4.2.1.1.4 Network 28
4.2.1.2 Data Integrity and Confidentiality 28
4.2.1.3 Audit Server (ARC) 30
4.2.1.4 Active Directory Domain Controller (ACD) 31
4.2.1.5 Security Domains (DOX) 32
4.2.1.6 Firewall Security Manager (NFM) 33
4.2.1.7 Domain Name System (DNS) 33
4.2.1.8 Intrusion Prevention System (IPS) 34
4.2.1.9 Radius & TACACS+ Services (NRS) 36
4.2.1.10 Key Management Service 38
4.2.1.11 Network Persistent Store (NPS) 39
4.2.1.12 KMNG Workstation 39
4.2.1.13 KMNG Operator 40
4.2.1.14 Key Server 40
4.2.1.15 Key Server Operator 40
4.2.1.16 Key Server Client 40
4.2.1.17 Key Server Resilience 41
4.2.1.18 Key Server Certificate 41
4.2.1.19 Key Server Access Control 41
4.2.1.20 Key Server RSA Key Set 41
4.2.1.21 Key Server Initialisation 41

UNCONTROLLED IF PRINTED

FUJ00232658

4.2.1.22 Remote Management and Recovery 41
4.2.1.23 Remote Monitoring 41
4.2.1.24 SSL 42
4.2.1.25 CHAP 42
4.2.1.26 PIN Management 42
4.2.1.27 Counter 42
4.2.1.28 Hardware Security Module (HSM) 42
4.2.1.29 PIN Pads 42
4.2.1.30 Root Certification Authority (CA) 43
4.2.1.31 Secure Configuration Assistant (SCA) 43
4.2.1.32 Money Gram Password 43
4.2.1.33 BAL Oracle User Password 43
4.2.1.34 Component Interaction 43
4.2.1.35 Branch Access Layer 44
4.2.1.36 Key Enforcement Policy 45
4.2.1.37 Key Change Synchronisation 45
4.2.1.38 Identity and Access Management Service 45
4.2.1.39 Secure Event Management Service 46
4.2.1.40 Vulnerability Management Service 47
4.2.1.41 Payment Card Industry Solution (PCI) 47
4.2.1.42 Bluecoat (Reverse Proxy Service) 48
4.2.1.43 HBS- Web Server 51
4.2.2 System Management Service (SMS) 53
4.2.2.1 Service Summary 53
4.2.2.2 Service Availability 54
4.2.2.3 SYSMAN3 Overview 54
4.2.2.4 Tivoli Management Framework (SYSMAN) 54
4.2.2.5 System Management Platforms 55
4.2.2.6 Event & Systems Monitoring 56
4.2.2.7 Fujitsu Network Management Systems (NMS / NNM) 57
4.2.2.8 Real Time Active Dashboard (RAD) 58
4.2.2.9 Software Distribution and Asset Management 58
4.2.2.10 Remote Access and Diagnostics 61
4.2.2.11 Time Synchronisation 64
4.2.2.12 High Level Scheduling 65
4.2.2.13 Enterprise Boot Server (EBS) 66
4.2.2.14 Server Provisioning 67
4.2.2.15 Service Monitoring 68
4.2.2.15.1 Active Monitoring 68
4.2.2.15.2 Passive Monitoring 68
4.2.2.15.3 Event Processing 68
4.2.2.16 Branch Agent 69
4.2.2.17 Campus Agents 69
4.2.2.18 Related Actions 70
4.2.2.19 Event Management Infrastructure 70
4.2.2.20 Branch Counter 70
4.2.2.21 Branch Router Events 72
4.2.2.22 Campus Events 72
4.2.2.23 Links to Known Error Logs (KELs) 74
4.2.2.24 Related Actions 74
4.2.3 Operational Business Branch Change (includes OBC) Management / Estate Management Service 74
4.2.3.1 Branch Change Management (includes OBC) Overview 74
4.2.3.2 Estate Management Overview 75
4.2.3.3 Main Components 75
4.2.3.4 Estate Management Systems 77
4.2.3.5 Estate Management Operations 78

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.3.6 System Operations 78
4.2.3.7 Estate Management interfaces 79
4.2.3.8 Estate Management Server (EST) 79
4.2.3.9 EST Endpoints 80
4.2.3.10 EST Endpoint Clients 80
4.2.3.11 Boot Platform 80
4.2.3.12 Boot DMZ 81
4.2.3.13 MTAS Access 81
4.2.3.14 Scheduler Functions for Estate Management 81
4.2.4 Reconciliation Services 81
4.2.4.1 Management Information Services (MIS) Overview 82
4.2.4.1.1 MIS Clients 82
4.2.4.2 The Data Reconciliation Service (DRS) 82
4.2.4.2.1 Reconciliation Reporting – HNG-X Outlets to DRS 83
4.2.4.2.2 Reconciliation Reporting – POA DRS to PO Ltd 83
4.2.4.3 Data Warehouse 84
4.2.5 End to End Reconciliation Service 87
4.2.6 POLSAP Development and Test/QA Services 87
4.2.6.1 POLSAP Hosting Development Service 88
4.2.6.2 POLSAP Hosting XI QAtest Load Service 88
4.2.6.3 POLSAP Hosting QATest Archive Service 89
4.2.7 Network Services 89
4.2.7.1 Branch Network Service 89
4.2.7.2 Branch Network Service 89
4.2.7.2.1 Time to Repair 90
4.2.7.2.2 Maintaining Contact with the HNG-X Central Infrastructure 91
4.2.7.3 Branch Service Structure 91
4.2.7.4 Client Links 92
4.2.7.5 The Branch Resilient Network (BRN) 93
4.2.7.6 Branch Router Overview 93
4.2.7.7 Branch Network Overview 94
AEI Interim Branch Connectivity 95
4.2.7.8 Wireless WAN Service 96
4.2.7.9 Data Centre LANs 97
4.2.7.10 WAN Connectivity - Fujitsu sites to IRE11 & IRE19 Data Centre 98
4.2.8 Fujitsu Shared Services 98
4.2.8.1 Shared Data-centres 98
4.2.8.2 TRIOLE for SERVICE (TfS) – Shared Incident Management System 98
4.2.8.3 ConnectDSL – Shared Service - SDC / TCY 99
4.2.8.4 Fujitsu Global Cloud Platform(Salesforce) 99
4.2.8.5 Cloud Connect VPN service and Cloud connect network service. 100

NETWORK SUB-SYSTEM DESCRIPTION: 100

4.2.9 External Suppliers 103
4.2.9.1 VODAFONE Network 103
4.2.9.2 Transaction Network Services (TNS) 103
4.2.9.3 Talktalk Business 104
4.2.9.4 EMC – Disk Storage Supplier 104
4.2.10 Data Centre Operations Service 104
4.2.11 Support Services 105
4.2.11.1 The System Management Centre (SMC) 105
4.2.11.2 POA Customer Service 105
4.2.11.2.1 Reference Data Team (RDT) 106
4.2.11.2.2 Third Line Support Services (SSC) 106
4.2.11.2.3 Reconciliation Service 107
4.2.11.2.4 Management Information Systems (MIS) 107

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.11.2.5 Service Introduction (SI) ... 107
4.2.11.2.6 Change Control ... 107
4.2.11.2.7 Configuration Management – Signing Server. ... 107
4.2.11.2.8 Live System Team ... 108
4.2.11.2.9 Fourth Line Support ... 108
4.2.12 Operational Services sub-group ... 108
4.2.12.1 The Systems Operate Service ... 108
4.2.12.1.1 UNIX System Support Service ... 110
4.2.12.1.2 Database Support Service ... 111
4.2.12.1.3 Windows NT / WINTEL Support Service ... 111
4.2.12.1.4 Systems Security Team ... 112
4.2.12.2 Network Support Services ... 112
4.2.13 The Major Account Controllers (MAC) ... 113
4.2.13.1 Overview ... 113
4.2.13.2 Communications Management Team (CMT) ... 113
4.2.13.3 Major Account Controllers (MAC) ... 114
4.2.13.4 Electrical Power ... 115
4.2.14 The Message Broadcast Service (MBS) ... 115
4.2.14.1 Service Availability ... 115
4.2.15 Service Integration Service ... 115
4.2.16 Receipt Template Service ... 115
4.2.17 Service Management Service ... 116
4.2.17.1 Service Elements ... 116
4.2.17.2 Loss of primary operational office site in Bracknell ... 117
4.2.18 Internet Data Exchange (DXI) ... 117
4.2.19 Corporate Data Exchange (DXC) ... 117
4.2.20 Performance & Capacity Management (SPN) ... 119
4.2.21 Branch Support Database System (BRSS) ... 121
4.2.21.1 Overview ... 121
4.2.21.2 Data Population ... 123
4.2.21.3 Support Interface ... 123
4.2.21.4 Resilience / Fail-over ... 123

5 TESTING STRATEGY ... 124

5.1 Initial Testing ... 124
5.2 Ongoing Test Strategy ... 124

6 PREVENTATIVE MEASURES ... 125

6.1 Major Account Controllers (MAC) DR facility ... 125
6.2 Triole for Service (TfS) – Service Desk system ... 125
6.3 Data Centre Operations Services (IRE11 / IRE19) ... 125
6.3.1 Environment Monitoring Facilities ... 126
6.3.2 Data Centre Air Conditioning – IRE11 & IRE19 ... 126
6.3.3 Data Centre Power – IRE11 & IRE19 ... 126
6.3.4 Oracle Real Application Cluster (RAC) ... 127
6.3.5 Oracle DataGuard ... 127
6.3.6 Disk Storage Arrays ... 128
6.3.7 SAN Fabric ... 128
6.3.8 Host Systems ... 128
6.3.9 Blade Frame and Storage Overview ... 129
6.3.10 BladeFrame Connections ... 131
6.3.11 BX900/PAN7 ... 132
6.3.12 Salesforce Support Service ... 133
6.4 Network Services ... 135
6.4.1 Network Capacity into Data Centres ... 135

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6.4.2 Data Centre Network Topology 135
6.4.3 Data Centre Disaster Recovery (DR) - Network 137
6.4.4 Fujitsu Network Management Systems (NMS / NNM) 139
6.4.5 Vodafone Network Management Centre 139
6.4.6 Vodafone ISDN Availability 139
6.4.7 Fujitsu Services SDC01 & TCY01/02 Data Centres & ADSL Service 139
6.4.8 Wireless WAN Availability 139
6.4.8.1 Orange Wireless WAN - Availability & Resilience 140
6.4.8.2 Branch Router Availability 140
6.4.9 Transaction Network Services UK LTD (TNS) 140
6.4.10 Post Office Limited Northern Data Centres 140
6.5 The Security Service 140
6.5.1 Key Management Servers and Database – HNG-X 140
6.5.2 KMNG Workstations 140
6.5.3 Tivoli Infrastructure 141
6.6 Branch and Estate Change Management Recovery and Resilience 141
6.6.1 Estate Management Database Server (EST) 141
6.6.2 Boot Platform 141
6.6.3 Branch Change Management Server (BCMS) 142
6.6.4 Radius Authentication 142
6.6.5 Hardware Resilience for Estate Management Platforms 142
6.6.6 EMDB Database Backups 142
6.7 Reconciliation Service 142
6.7.1 Main Host / Data Warehouse 142
6.7.2 Main Host Server Resilience 143
6.8 POLSAP Development and Test QA Services – IRE19 143
6.9 System Management Service 143
6.9.1 System Management Platforms – Resilience 143
6.9.2 Loss of Network Communications to IND49/STE04 144
6.9.3 Buildings – Blackpool BLA01 – MSS North/ SMG 144
6.9.4 Buildings – IND49 - SMC 144
6.9.5 People - MSS 144
6.9.6 People – SMC in IND49 144
6.10 Operational Support Services 144
6.10.1 The Systems Operate Service 144
6.10.1.1 Activation 144
6.10.1.2 Loss of Documentation server 145
6.10.1.3 Loss of Electrical Power 145
6.10.1.4 Loss of Telephone exchange 145
6.10.1.5 Loss of the IRE11 Office area 145
6.10.2 Support Services 145
6.10.2.1 The System Management Centre (SMC) 145
6.10.2.2 POA Customer Services - Overview 145
6.10.2.2.1 Incident Management 146
6.10.2.2.2 Peak Support Incident Management 146
6.10.2.3 Configuration Management – Signing Server 146
6.10.2.3.1 Change Control 146
6.10.2.3.2 Development Operational Support Live System Team (LST) 146

7 PREPAREDNESS MEASURES 148

7.1 Testing 148
7.2 Service Management & Delivery 148
7.3 Risk Analysis 148

8 CONTINGENCY MEASURES 149

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

8.1 Recognition 149
8.2 Activation 149
8.3 Incident Management 149
8.4 Initiation of Recovery Procedures 149

9 RECOVERY OF NORMAL SERVICE 151

9.1 Recovery Time Objectives and Recovery Point Objectives 151
9.1.1 HNG-X Infrastructure RTO and RTP Objectives 151
9.1.2 HNG-X Services Disaster Recovery RTO and RPO Objectives 153

10 IMPACT & RISK ASSESSMENT 155

10.1 Risks Identified Against the HNG-X Support Services 155
10.2 Trigger Tables for HNG-X Support Services 157

11 RISKS IDENTIFIED AGAINST MAJOR ACCOUNT CONTROLLERS (MAC) . 210

11.1 Trigger Tables for Major Account Controllers (MAC) 210

12 SUMMARY OF CONTINGENCY ACTIONS 223

12.1 Summary of Contingency Actions for HNG-X Support Services 223
12.1.1 Reconciliation Service 223
12.1.2 Security Management Service 223
12.1.3 Branch Change Management Service 223
12.1.4 Estate Management Service 223
12.1.5 Network Services 223
12.1.6 Data Centre Operations Service 223
12.1.7 SAP Development and QA-Test Systems 223
12.1.8 System Management Service 223
12.1.9 Support Services 223
12.1.10 System Operate Services 224
12.1.11 Reference Data Management Service 224
12.1.12 Service Integration Service 224
12.1.13 Receipt Template Service 224
12.1.14 Service Management Service 224
12.2 Summary of Contingency Actions for the MAC 224
12.2.1 BT Telephone Call Delivery System, via IVR (NBSC), to MAC. 224
12.2.2 Loss of Functionality in STE04 for MAC 224
12.2.3 People 225
12.2.4 Manual Processes due to total loss of TfS Incident Management System 225
12.2.5 Loss Of access to Tivoli / KMA / Global User Counter / One Shot Password System 225
12.2.6 Loss Commander – Call Management 225

13 POST OFFICE LIMITED FAILURES IMPACTING POA SERVICES 226

13.1 Post Office Limited failures impacting POA RDMS Service 226
13.2 POL and AP Client failures impacting POA APS Service 226
13.2.1 Post Office Limited 226
13.2.2 AP Clients 226
13.3 Post Office Ltd failures impacting POA TPS Service 226
13.4 Post Office Ltd and Supplier failures impacting POA NBS Service 226
13.5 Post Office Ltd and Supplier failures impacting POA DCS Service 226

14 PLAN ACTIVATION 228

14.1 Major Business Continuity Incident (MBCI) 228

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

14.2 Site Failover 228

15 CONTACT LIST 230

15.1 Normal Processes 230
15.2 Escalation Processes 230

16 APPENDICES 233

16.1 Appendix One: Post Office Outlet Trigger Table 233
16.2 Appendix 2 IRE11 – IS Data Centre Information 234
16.3 Appendix 2 IRE19 – IS Data Centre Information 234

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

0.2 Document History

Version No.	Date	Reason for Issue	Associated CP/PinICL
0.1	05/12/08	Initial draft. Sent out for Technical review	None
0.2	23/01/09	Updated Draft following restricted comment cycle	None
0.3	09/04/09	Updated by Nigel Bailey following comments on draft version and request for additional content from Tony Wicks Format and layout corrections	None
0.4	09/04/09	Tidy up by Tony Wicks before sending out on comment cycle	None
1.0	27/10/09	Updated personnel mentioned along with comments received through internal document review.. Also updates in line with internal audit. Input from Vic Lawson and Nigel Hatcher regarding audit updates.	
1.1	26/11/10 27/05/11	Reviewed and updated Reconciliation Service sections with Claire Drake Replaced refs of POLFS with POLSAP Removed majority of references to Wigan Removed refs to SMC bridging Updated doc to reflect SMG/MSS location as BLA01 Changed refs of Bangalore to IND44 Changed refs of MAC to IMT Added mention of POA Networks now residing at WAR07. Added new info about laptops held by EMS for DR purposes. Added risk for loss of CRE02 Improved structure of trigger tables including addition of an index table.	None
1.2	06/06/11	Created version1.2 for formal review cycle based upon changes made in sub versions up to and including v1.1.2 (see v1.1 changes)	None
1.3	01/05/2/13 14/8/2014	Added POMS (section 4.2.7.6) & Blue coat (Reverse proxy server). Document updated for formal Review. Also SSC comments updated.	None
1.4	07/10/14	Updates in response to review comments	None

UNCONTROLLED IF PRINTED

0.3 Review Details

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Review Comments by :	19-Sep-2014
Review Comments to :	Changdev Pawashe & Post Office Account Document Management
Mandatory Review	
Role	Name
POA MAC SDM	Sandie Bothick
POA Networks SDM	Roger Stearn
POA SAP & Online services	Gaby Reynolds
Credence SDM	S Edmondson
POA Client Services Manager (Engineering, OBC)	Leighton Machin; Chris Harrison
POA Security SDM (includes Reconciliation, Key Management)	Kumudu Amaratunga
Infrastructure Operations SDM	Andrew Hemingway
Incident & Problem Management SDM	Steve Bansal
SSC Manager	Steve Parker; SSC Duty Manager
System Owner	Andy Gibson / Ed Ashford / Paul Stewart / Joe Diffin
Optional Review	
Role	Name
POA Senior Operations Manager	Alex Kemp
POA Solutions Architect	Krishnaraj Selvaraj
POA Service Transition and Change	Tony Atkinson
SMC Manager	Jacob Cherian
Networks Architect	Steve Freke; John A Clarke
Architect	Jason Clark
HNS Networks Manager	Raj Patel
MSS/ SMG Operations Manager	Jerry Acton
NT Management	Ian Gibson
IRE11/ IRE19 Datacentre Operations Manager	John Hill
Problem Manager	Steve Gardiner
Problem Manager	Tony Wicks
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name

UNCONTROLLED IF PRINTED

(*) = Reviewers that returned comments

0.4 Associated Documents (Internal and External)

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Reference	Version	Date	Title	Source
ARC/APP/ARC/0005			HNG-X Online Services Architecture	Dimensions
ARC/APP/ARC/0007			HNG-X Batch Applications Architecture	Dimensions
ARC/SEC/ARC/0003			HNG-X Technical Security Architecture	Dimensions
ARC/SYM/ARC/0001			System and Estate Management – Overall Architecture	Dimensions
ARC/SYM/ARC/0003			HNG-X System and Estate Management Monitoring	Dimensions
ARC/SYM/ARC/0005			HNG-X Estate Management Component Architecture	Dimensions
CON/MGM/005 (BP/DOC/021)			Post Office Limited and Fujitsu Services Business Continuity Interface Agreement	Post Office Limited
DES/APP/HLD/0007			DCS Authorisation Agent High Level Design	Dimensions
DES/APP/HLD/0012			DVLA Internal Web Service High Level Design	Dimensions
DES/APP/HLD/023			Branch Support Database High Level Design	Dimensions
DES/APP/HLD/0030			Audit Data Collection & Storage High Level Design	Dimensions

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Reference	Version	Date	Title	Source
DES/APP/HLD/033			Data Reconciliation Service High Level Design	Dimensions
DES/APP/HLD/0082			Data Warehouse High Level Design	Dimensions
DES/MIG/HLD/0004			POL FS – Migration HLD	Dimensions
DES/NET/HLD/0006			Domain Name System	Dimensions
DES/NET/HLD/0018			Corporate Data Exchange Proxy High Level Design Specification	Dimensions
DES/PER/HLD/0002			HNG-X - Capacity Management Database High Level Design	Dimensions
DES/PPS/HLD/0003			Active Directory High Level Design for HNG-X	Dimensions
DES/PPS/HLD/0024			HNG-X Datacentre Platform Foundation Bootstrap HLD	Dimensions
DES/SEC/HLD/0003			HNG-X Key Management High Level Design	Dimensions
DES/SYM/HLD/0001			MON Supporting Platforms	Dimensions
DES/SYM/HLD/0002			MON Supporting Agents	Dimensions
DES/SYM/HLD/0014			SYSMAN3 User Access	Dimensions
DES/SYM/HLD/0034			SYSMAN3 - Backup, Availability and Disaster Recovery High Level Design	Dimensions
DES/SYM/HLD/0036			SYSMAN3 - Branch Router Management	Dimensions
DES/SYM/HLD/0048			Tivoli Real Time Active Dashboard – Business Process Views	Dimensions
DEV/INF/LLD/0047			Internet Access LLD	Dimensions
DEV/INF/LLD/0051			Low Level Design for McAfee Intrushield IDS/IPS Appliance	Dimensions
DEV/INF/LLD/0077			Radius and TACACS+ Platform – Low level design	Dimensions
DEV/INF/LLD/0080			Branch Router Wireless WAN Service Network	Dimensions
DEV/INF/LLD/0083			HNG-X Vulnerability Scanner Low Level Design	Dimensions

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Reference	Version	Date	Title	Source
DEV/GEN/SPE/0007			Platform Hardware Instance List	Dimensions
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office AccountHNG-X Document Template	Dimensions
SVM/SDM/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Service Business Continuity Plan	Dimensions
SVM/SDM/PLA/0003			HNG-X Business Continuity Operational Test Plan	Dimensions
SVM/SDM/PLA/0030			HNG-X Engineering Service Business Continuity Test Plan	Dimensions
SVM/SDM/PLA/0031			HNG-X Security Business Continuity Test Plan	Dimensions
SVM/SDM/PRO/0028			Fujitsu Services POA Customer Service HNG-X Business Continuity Management Process	Dimensions
SVM/SDM/SD/0014			OBC Branch Change Service	Dimensions
SVM/SDM/SD/0020			End to End Reconciliation Reporting	Dimensions
SVM/SDM/SD/0019			Communications Management Team: Service Description	Dimensions
SVM/SDM/SD/0022			Receipt Template Service: Service Description	Dimensions
SVM/SDM/SD/0007			Service Management: Service Description	Dimensions
SVM/SDM/SIP/0001			HNG-X Business Continuity Framework	Dimensions

UNCONTROLLED IF PRINTED

0.5 Abbreviations

Abbreviation	Definition
[A]	Authorisation
[C]	Confirmation
[F]	Financial Advice Note

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Abbreviation	Definition
[R]	Request
AAC	Application Authentication Cryptogram – generate by the ICC as a result of a failed transaction
ACS	Auto-Configuration Service
ADSL	Asymmetric Digital Subscriber Line
AEI	Application Enrolment and Identity (AEI) service
AIS	Application Interface Specification
AP-ADC	Automated Payments-Advanced Data Capture
APOP	Automated Payments Out-Pay
APS	Automated Payments Service
BAL	Branch Access Layer
BCM	Business Continuity Manager
BCMS	Branch Change Management System
BCMT	Business Continuity Management Team
BCT	Business Continuity Team
BDC	Bureau de Change Service (or Backup Domain Controller)
BGP	
BNR	Branch Network Resilience
BRDB	Branch Database
BCDB	Branch Configuration Database (HNG-X solution)
BCMS	Branch Change Management System – HNG-X replacement for OBC and OCMS
BRSS	Branch Support Database
BT	British Telecom
VODAFONE	Cable & Wireless
CAPO™	Card Account for Post Office
CE	Customer Edge (Cable & Wireless Router)
CHAP	Challenge Handshake Authentication Protocol
CI	Card Issuer
CSM	Content Switch Module
CSS	Contents Services Switch
CTF	Critical Time Factors
DCS	Debit Card System
DCSM	Debit Card System Management (server)
DCOS	Data Centre Operations Service
DNS	Domain Name Server

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Abbreviation	Definition
VODAFONE	Cable and Wireless
DMZ	De-Militarised Zone
DRS	Data Reconciliation Service
DSLAM	Digital Subscriber Line Access Multiplexor
DTF	Daily Transaction Feed
DVLA POME	Department of Vehicle Licensing Authority – Post Office MOT Enquiry
DXC	Corporate Data Exchange
PODG	Post Office Data Gateway
EDS	Electronic Data Systems
EMDB	Estate Management Database Branch Change Management System
EMV	Europay MasterCard Visa standard for financial smart cards.
EoD	End of Day
EPOSS	Electronic Point of Sale Service
EST	Estate Management Server
ETS	Electronic Top-up Service
FDDI	Fibre Optic Distributed Database
FI	Financial Institution
FJCS	Fujitsu Services Core Services
FRTS	First Rate Travel Service
FSCS	Fujitsu Services Core Services
FTMS	File Transfer Management Service
GPS	Global Positioning System
GSN	Global Satellite Network
HBS	Horizon Business Server
MAC	Major Account Controllers
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICC	Integral Chip Card
IP	Internet Protocol
IPS	Intrusion Prevention System
KEK	Key Encryption Key
KES	Key Encryption Seed
KM	Key Management
KMA	Key Management Application
KMC	Key Management Controller

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Abbreviation	Definition
KMS	Key Management System
LAN	Local Area Network
LAR	Logical Access Router
LCR	Logical Campus Router
LFS	Logistics Feeder Service
LNS	L2TP Network Server
MBCI	Major Business Continuity Incident
MBS	Message Broadcast Service
MID/TID	Merchant Identifier/Terminal Identifier
MIS	Management Information Service
MoT	Ministry of Transport (Roadworthiness Certificate)
MTAS	Mid Tid Allocation Service
NBR	Network Branch Resilience
NBS	Network Banking Service
NBSC	Network Business Support Centre operated by Post Office
NBX	Network Banking Service (Replacement)
NDC	Northern Data-Centre (Post Office Limited Operated)
NPS	Network Persistent Store
NNM	Network Node Manager
NMS	Network Management System
NS&I	National Savings and Investment
NSSC	National Secure Stock Control
NST	Network Service Type
NTP	Network time protocol
O/S	Operating System
OBC	Outlet Business Change
OCMS	Outlet Change Management Service
OPS	Outlet Processing System
PAF	Postal Address File
PES	Personal Earth Station
PFG	Payment File Generator
PHU	Portable Hosted Unit (counter)
PIN	Personal Identification Number
POL	Post Office Limited
POLSAP	The POLSAP application that is configured by Fujitsu from SAP, to meet

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Abbreviation	Definition
	the business needs of Post Office.
POMS	Post Office Managed Switch
POP	Point Of Presence
PPP	Point to Point Protocol
RAB	Release Authorisation Board
RAC	Request, Authorisation, Confirmation Model
RAC (Oracle)	Oracle Real Application Cluster. The full term has been used rather than the abbreviated "RAC" as this might be confused with the Network Banking Request Authorise Confirm model.
RACF	Request, Authorisation, Confirmation with Financial Advice Note
RAD	Real time Active Dashboard
RD	Reference Data
RDMC	Reference Data Management Centre
RDMS	Reference Data Management Service
RDS	Reference Data System
RMG	Royal Mail Group
POA	Post Office Account
SAS	Secure Access Server (SSN)
SMC	Systems Management Centre
SMS	System Management Service
SOAP	Simple Object Access Protocol
SORN	Statutory Off the Road Notification
SOS	Systems Operate Service
SSC	Software Support Centre
SSL	Secure Sockets Layer, (also referred to as HTTPS)
T&T	Track and Trace
TC	Transaction Certificate
TDES	Triple Data Encryption Standard
TES	Transaction Enquiry Service
TFS	TRIOLE For Service
TH1	Tech Hall 1
TH2	Tech Hall 2
TIP	Transaction Information Processing
TLSS	Terminal Server Licensing server
TMR	Tivoli Managed Region
TMS	Transaction Management Service

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Abbreviation	Definition
TPM	Tivoli Provisioning Manager
TPS	Transaction Processing Service
TNS	Transaction Network Services
TWS	Tivoli Workload Scheduler.
UTC	Coordinated Universal Time
VED	Vehicle Excise Duty
VOSA	Vehicle and Operations Services Agency
VPN	Virtual Private Network
WAN	Wide Area Network
XML	Extensible Markup Language

0.6 Glossary

Term	Definition
Hydra	Is the period between the first step of the Data Cente migration (currently the POL FS move) and the last Horizon branch being migrated to the Branch Database.
Luggable/PHU	A Portable Horizon PC system (also known as a "mobile")
PGDD Service Application	The Guaranteed Delivery Date application which interacts with Neopost
Till	A term for any Terminal or Kiosk connected to HBS and so differentiated from a Horizon Counter.

UNCONTROLLED IF PRINTED

0.7 Changes Expected

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Changes
This is an operational document, which will be amended for numerous reasons including: • New risks identified; • Improved or new contingency actions are identified; • Operational changes to the HNG-X Supporting Services Infrastructure. 1. To avoid duplication some sections that cover services or equipment used for primary and support services are only covered in SVM/SDM/PLA/0002 – may need to review after draft reviews 2. Section 11 & 11.1- Risk Identified & trigger table will needs to be updated. Horizon Service Desk is no longer exist. This sections will need to udated with details of MAC team. Awaitng to get the MAC Service description document. 3. Section 12.2 Summary of Contingency Actions for the MAC will needs to be updated. Awaitng to get the MAC Service description document. 3. Section 9.1- Recovery Point Objectives wil need to be updated."Normal Service Provision" is meaningless for an RPO. To update RPO's will need to check with platform owners. 4. Section 4.2.13.3 Major Account Controllers (MAC) & Section 4.2.13.4 Voice Systems Features will need to be updated after getting the MAC Service description document. 5. Services which are migrating to FCN will need to be update. 6. Section 4.2.9.4 & section 6.3.6 will need to be updated after completion of Belfast refresh programme. 7. Section 9.1.1 & 9.1.1 RTO will need to be updated after getting the information from all the platform owners. This will cover the comment19 which is received from Edward Ashford.

Commented [ML1]: Is this still not complete?

UNCONTROLLED IF PRINTED

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.

.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

1.0 Introduction

1.1 Using this document

This Business Continuity Plan has been created for the services that support the Post Office HNG-X services provided from IRE11 and IRE19.

1.2 Business Continuity Plans for HNG-X

For HNG-X the following Business Continuity plans have been created:

1. HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002);
2. HNG-X Support Services Business Continuity Plan (SVM/SDM/PLA/0001 - this document);
3. HNG-X Engineering Business Continuity Plan (SVM/SDM/PLA/0030)
4. HNG-X Security Business Continuity Plan (SVM/SDM/PLA/0031)

This Contingency Plan provides a summarised description of the overall Operational HNG-X Support Service provided by Fujitsu Services. This includes the following sub-services:

- Security Management Service
- Branch Change Management Service
- Estate Management Service
- Network Services
- Data Centre Operations Service
- SAP Development and QA-Test Systems
- System Management Service
- Support Services
- System Operate Services
- Reference Data Management Service
- Reconciliation Service (includes Management Information Services, and the Data Warehouse, End to End Reconciliation
- Service Integration Service
- Receipt Template Service
- Major External Supplier Services
- Service Management Service
- POA Programme and Development Operational Support
- MAC (Major Account Controllers) (includes the Communications Management Team)
- Message Broadcast Service
- GWS- Generic Web Services
- PODG- Post Office Data Gateway

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

This document describes the measures taken by Fujitsu Services to minimise the risk of POA being unable to provide these services and it explains the actions the Problem, Service, or Business Continuity Manager takes to instigate service recovery.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

2 Scope

This plan covers the following key areas.

- A summary of the individual HNG-X support services
- A summary of the testing activities undertaken to validate those services.
- The measures taken to anticipate and plan for business continuity incidents
- A risk and impact assessment
- Agreed trigger points for plan activation
- References to relevant operational recovery processes
- Problem management contacts and escalation points

This plan does not provide detailed operational procedures with regard to recovery. Further details on the procedures for recovery can be found in the Fujitsu Services Core Services Operations Procedures Manual Index (SU/MAN/018).

3 Ownership and Operation

The Fujitsu Services Post Office Account Infrastructure and Availability Manager is the owner of and is responsible for the maintenance and operational verification of this document. The Fujitsu Services Core Services Service Manager operates this plan. Contact details are shown below.

MAC /CMT Business Continuity is also included within this plan.

Name	Position	Office Contact No.	Out of hours No.	Services Covered
Alex Kemp	Fujitsu Services, Post Office Account, Head of Service Operations.			All
Changdev Pawashe Post Office Account(Deputy)	Fujitsu Services, Post Office Account, Business Continuity Manager.			All
Sandie Bothick	Service Delivery Manager (MAC)			MAC
Helen Robinson	Fujitsu Services Stream Manager (MAC)			MAC

The Fujitsu Services POA Business Continuity Manager and the Service Managers within Fujitsu Services POA Customer Service Operations, responsible for service availability, hold copies of this plan.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4 Service Functionality

4.1 Services Overview

For the purposes of Business Continuity planning, this contingency plan has been produced to document the Post Office Accountresponsibilities for the end to end HNG-X support services. From an operational perspective it is impracticable for the plans to cover every element or component in the end-to-end service, e.g. an unserviceable power lead in a single counter outlet, however major components are documented in the risk table section 11.2 of SVM/SDM/PLA/0002.

Figure 1 provides an overview of all the HNG-X Services for which POA has partial or full responsibility.

This figure is derived from the Business Continuity Framework SVM/SDM/SIP/0001 and is based upon the contractual requirement defined in 'The Agreement' that the Business Continuity plans shall document the Applicable Services. The abbreviations used for those services are defined in SVM/SDM/SIP/0001. Also note that LFS refers to the full end to end service.

It is emphasised that some hardware components such as the Main Host (Database Server), EMC Disc array and Network Routers in the Data-centres deliver service to all the sub-services detailed in this plan. For some sub-services, there are hardware and software components specifically dedicated to that sub-service.

The details of risks to a service using only shared architecture can be found against individual infrastructure elements in the table in section 10 below and in the risk table section 11.2 of SVM/SDM/PLA/0002.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The diagram also provides details of the support applications and services covered within the HNG-X Services Business Continuity Plan SVM/SDM/PLA/0002.

HNG-x Services Overview

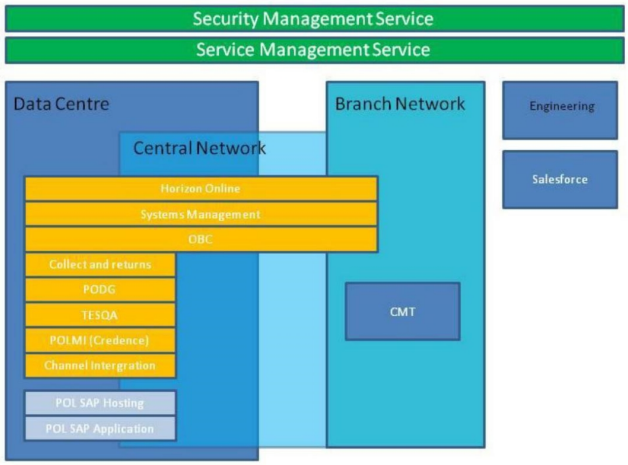


Figure 1

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.1.1 Infrastructure Sub-services

A number of IT sub-services are used to support the HNG-X services, however for the purposes of this plan they can be categorised into the following infrastructure support sub-services:

- The Security Service
- System Management Service
- The Outlet Change Management Service
- The Estate Management Service
- Reconciliation Service
- POL SAP (Development and QATest servers)
- Network Services (Vodafone and Transaction Network Services).

For the purposes of this continuity plan these sub-services can be considered to be running primarily from the infrastructure contained in the campuses (IRE11 & IRE19).

4.1.2 Operational Support Sub-Services

Additionally there are a number of HNG-X operational support sub-services:

These consist of a number of support teams:

1. The Major Account Controllers (MAC) who manages the incident transfers to the Atos Service Desk for issues in POL Clients domains. HSD is replaced by ATOS.
2. The System Management Centre(SMC) who, in addition to system management, provide second line technical support.
3. The Software Support Centre (SSC) who primarily provides third line support services.
4. Fourth line support is provided either by the Post Office AccountDevelopment team or by external suppliers, e.g. EMC or Microsoft.
5. The HNG-X service is also supported by number of operational units
6. The Core Services System Operate Service team who provide UNIX, NT and database operational expertise.
7. The System Management Centre operational event management team at IND49, MSS and SMG staff based at BLA01.
8. The POA Customer Service operational teams, i.e. providing Reference Data operational service, and the HNG-X Service Delivery Management functions.
9. The POA Programme and Development operational support teams.

4.2 Infrastructure Support Services

Figure 1 provides an overview of all the HNG-X Services for which POA has full responsibility, and identifies the support applications and services covered within this document SVM/SDM/PLA/0001.

4.2.1 The Security Management Service

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The Security Management Service provides a range of security-related activities that support the establishment and maintenance of an ISO 27001 compliant infrastructure. The Security Management Service monitors operations and introduces specific protective security controls to maintain the integrity, availability and confidentiality of information used and produced by the various Services, other than the Service Integration Service. See: ARC/SEC/ARC/0003

The risks to the infrastructure supporting the Security Management Service can be found in the trigger table in section 10 starting at row 14.

4.2.1.1 *Security Strategy*

The security strategy for HNG-X is risk based and uses the Prevention => Containment => Detection => Response model.

This strategy applies to both infrastructure and software development and provides defence in depth protection to the HNG-X system through the application of layered security controls.

This security architecture has been developed with the aim of ensuring that there are no single points of failure and that each area of risk has a number of technical and management controls working together to mitigate that risk.

Item	Description
Prevention	**Use a combination of security controls such as physical, network, platform and application access control, system hardening and vulnerability management to reduce vulnerability.**
Containment	**Constrains the spread of malware or malicious activity using various techniques and controls such as network segmentation, anti-malware controls and physical, network and platform access control.**
Detection	**Quickly detect the presence of malicious activity or malware in any domain of HNG-X through the use of anti-malware, intrusion detection and security event management controls.**
Response	**Automatic or manual incident response to mitigate the activity using pre-configured activities, intrusion prevention and incident response procedures.**

UNCONTROLLED IF PRINTED

To reduce complexity and implementation times, the approach taken for security applications and services is to use internal Fujitsu services when appropriate and to buy and integrate COTS products rather than develop them internally.

Specific exceptions to this rule have been made in the area of cryptography and key management where the Horizon solution has been redeveloped for the cryptographic API, (referenced in DES/SEC/HLD/0002), and a key management solution has been developed in the absence of commercial alternatives.

Each online system or device can be further subdivided into four additional layers and by using these it is possible to define both the functions that take place at that layer and the security strategy for each layer.

The four layers are;

4.2.1.1.1 Application

This is the data processing and presentation layer utilising the services provided by the software and by the other three layers of the model.

4.2.1.1.2 Data

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The Data Layer is responsible for the storage, integrity and management of application, platform and network information.

4.2.1.1.3 Operating System

The major operating systems in HNG-X are Windows 2003 Server, Windows 2008, Windows XP, Red Hat Enterprise Linux 4, Solaris 10 and, during Hydra, Windows NT4. A definitive list of the Platform Types and their associated operating systems is maintained in DEV/GEN/SPE/0007.

Following the security strategy of prevention, containment, detection and response, a specific Horizon-Online build, (the Platform Foundation), has been created.

The Platform Foundation is suitably hardened by following a policy of removing unnecessary software from the system, applying the latest relevant patches, and setting appropriate permissions contained in the following documents;

- Windows Server 2003 Security Guide {DES/PPS/MAN/0004}
- Red Hat Enterprise Linux 4 Security Guide {DES/PPS/MAN/0006}
- Solaris 10 System Administration Guide - Security Services {DES/PPS/MAN/0005}
- Windows Server 2008 Technical Security Architecture (ARC/SEC/ARC/0003)

4.2.1.1.4 Network

The network architecture provides facilities to securely transmit data, to provide remote access and to segment networks. In addition analysis and reporting facilities are provided to report against SLAs and to enable base-lining and trending to be performed.

The following facilities are supplied by the service;

- Provides secure network capabilities.
- Provides secure remote access facilities.
- Provides network segmentation.
- Enables network analysis and reporting.
- Controls and manages network access control.

Detailed information on the HNG-X network infrastructure is contained in the HNG-X Network Architecture {ARC/NET/ARC/0001}.

4.2.1.2 Data Integrity and Confidentiality

The Data Integrity and Confidentiality service ensures that confidential or sensitive data is adequately protected within the HNG-X system.

A Root Certificate Authority and subordinate Certificate Authority is created to manage and create Public Key Certificates for a number of purposes.

The Root CA is an Enterprise Root CA using Microsoft Software that creates the Root CA Key Pair. This is a self-signed key pair and the Live (IRE11) and Test (IRE19) environments use different Root CAs. The private key of this key pair is then used to sign other certificates to verify their authenticity. The public key of this key pair is distributed to the subordinate CAs and to any other end-point that requires it.

The Root CA key pair is generated by the CS Security Manager and the resulting Certificate is deployed over the network, to the relevant end-points. The end-points are defined in detail in the HNG-X Key Management High Level Design {DES/SEC/HLD/0003} document.

The Root CA is stored by the CS Security Manager in a physically secured Fujitsu location.

© Copyright Fujitsu Services Limited 2014

UNCONTROLLED IF PRINTED

FUJ00232658

The current end-points requiring the Root CA certificate are;

- Counter
- Counter Spare
- EMDB
- Boot Platform
- TES-QA Workstations

In addition to the other security controls mentioned in this document, OID restrictions are applied both on the Counter and in the Data Centre, to ensure that any attempted connection must use a valid certificate for that environment. Alerts and errors are reported through the event management system.

The public key certificate for the appropriate Root CA and the SSL certificate signing sub-CA is stored in the Counter certificate store. This technique means that it is easy to separate Live and Test environments as the SSL termination point and the Counter have been configured to only accept the appropriate certificate.

See the following documents for more information:

- DES/SEC/HLD/0003 covers the design of the key management system.
- DES/SEC/HLD/0001 covers the design of the strong two-factor authentication system.
- DES/SEC/HLD/0002 covers the design of the cryptographic API, (Crypto-API), and key management server, used by Banking authorisation agents, Debit and Credit Card authorisation agents, Audit workstations, Debit Card Management Server, Connect:Direct Gateway Server and the Key Management Workstations.

UNCONTROLLED IF PRINTED

Through the implementation of a Crypto-API on all systems that require access to key material, an application can request the appropriate key for its purpose and receives the key and passphrase/PIN value in a secure fashion.

The Crypto-API component communicates with a dedicated Key Server which contains all of the relevant passphrase or PIN material. The Key Server retrieves the appropriate key from a table in the Network Persistent Store database and returns both the key material and the passphrase.

4.2.1.3 Audit Server (ARC)

The Audit server is responsible for gathering Audit Tracks generated from a wide range of components of the HNG-X systems including: -

- Post Office Counters
- Systems Management Facilities
- Database Hosts (including the Reference Data System)
- PODG(Post Office data Gateways)
- System Scheduler logs

Audit Tracks (including the External Gateway Audit Tracks) are not automatically duplicated at each data centre. Files for these tracks are produced by each Audit Server and are exchanged between the two sites utilising the Inter-data centre link.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

An Audit server exists at each data centre and operate in an Active/Active configuration, Each audit server gathers audit tracks from their local data centre.

In normal post Hydra operation, audit tracks will only be generated and gathered on the Active campus.

If there is a complete failover of the HNG-X service to the DR data centre, the audit server at the DR data centre will take over responsibility for gathering audit data from all failed over machines.

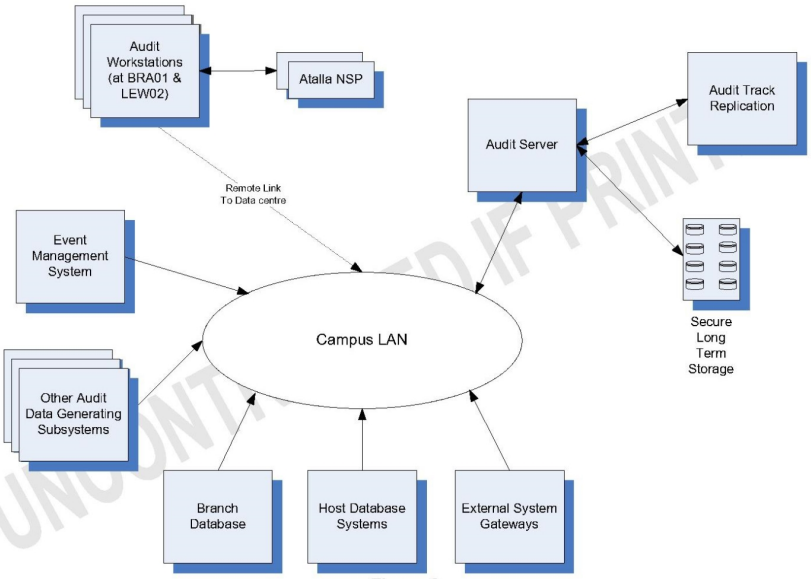


Figure 2

Major components of Audit Solution at a single data centre

4.2.1.4 Active Directory Domain Controller (ACD)

Active Directory is deployed as the central repository for user, computer, and network service-related information, and supports the existing industry standard, LDAP version 3 (LDAPv3), for querying and modifying information in the directory and provides the directory services for all Active Directory data centre servers, including the remote servers that will support the HNG-X infrastructure.

Active Directory is reliant upon the DNS for operation and uses the name resolution services provided by DNS to enable clients to locate Domain Controllers and enable domain controllers hosting directory services to communicate with each other.

The HNG-X Active Directory domain controllers will be hosted as para-Virtualised machines on the Active/Active Bladeframe pair in both data centres. The Bladeframe systems present the domain controllers as virtual sets of servers that exist in the SAN.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Active Directory is designed to be fault tolerant and can continue to operate if individual servers are unavailable for periodic maintenance.

4.2.1.5 *Security Domains (DOX)*

There are a number of defined security domains with the HNG-X security model; therefore data traffic will always be either intra-domain traffic or inter-domain traffic.

•Intra-domain traffic – Data traffic moving between systems in the same domain.

•Inter-domain traffic – Data traffic moving between systems in different domains.

There is a third class of traffic consisting of data moving into and out of the HNG-X infrastructure.

Intra-domain traffic may be unrestricted because the systems share a LAN segment, or may be restricted through the implementation of logical separation, (using VLANs), or physical separation, (using separate network segments in the same domain).

Inter-domain traffic must pass through an enforcement point that restricts data flow based on its source, destination, protocol, port, type or content/format.

Domains can also span physical locations. For example, the Key Management Domain contains Data Centre systems as well as workstations in remote locations such as Bracknell and Lewes.

In the event that a database or application, nominally in one tier, shares a platform with another database or application in a different tier, then the most restrictive set of permissions shall apply. This is particularly relevant to the Solaris Main Host that supports a number of Oracle Databases, some of which contain cardholder data and some of which don't. The Solaris Main Host has therefore been placed in the Core PCI-CE Domain in Tier 3, despite the fact that a number of Databases hosted on it do not store Cardholder Data.

The domain model is an overlay for each environment.

Separation between environments is controlled using a combination of preventive and detective controls such as access control, firewall rules, BladeFrame configuration, switch configuration and event monitoring.

The HNG-X Platform Hardware Instance List {DEV/GEN/SPE/0007} contains a definitive mapping of platform instances to security domains.

The following table describes the purpose of each security domain;

#	Name	Description
1	Core PCI-CE Domain	HNG-X Database Platform Types that store, process and transmit encrypted and hashed PANs.
2	Key Management Domain	HNG-X Platform Types that manage cryptographic material.
3	Infrastructure Support Services Domain	HNG-X Platform Types that manage and control the infrastructure, such as Active Directory and DNS Servers.
4	Horizon Domain	Virtualised retiring Horizon Platform Types
5	Support Services Domain	HNG-X Platform Types responsible for the management of Audit Data.
6	RDT Domain	Reference Data Team testing environments

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

7	Client Agents Domain	HNG-X Platform Types responsible for communication with Post Office clients.
8	Corporate / RMG Connection Domain	HNG-X Platform Types responsible for communication with the Fujitsu Corporate network and with the Royal Mail network.
9	Internet Connection Domain	HNG-X Platform Types responsible for communication across the Internet.
10	Support Connection Domain	HNG-X Platform Types responsible for managing support connections
11	Branch Connection Domain	HNG-X Platform Types responsible for Branch communication and management

There are 5 virtual Domain Controllers in each Data Centre running on RX300 servers.

4.2.1.6 *Firewall Security Manager (NFM)*

The Cisco Security Manager is used to manage firewalls and other security devices such as IOS routers which includes IPSEC VPNs and runs on the Firewall Security Manager Server (NFM), along with CiscoWorks, it provides centralised, auditable management, and minimises the security risk of changes being implemented on a firewall undetected.

This application administers consistent firewall policies using the policy view feature of the application.

Creation of the policies and their deployment to the ASAs and VPN applied routers is also managed from this server and is located within the Management Services LAN.

4.2.1.7 *Domain Name System (DNS)*

A DNS service is introduced to centralise name, IP address and service resolution and remove the dependency on individual platform host files. .

Almost all data centre and network infrastructure systems are expected to use DNS. DNS is a distributed hierarchical database system supporting the storage and dissemination of data. The data stored is typically device names (*terminal domains* in DNS terminology) and Internet Protocol (IP) addresses, however, many other types of data may be stored.

Typical DNS transactions are:

- Clients requesting the IP address of a given domain name (a *forward* lookup);
- Clients requesting the domain name of a given IP address (a *reverse* lookup);
- Dynamic registration of an IP address by a DNS client system;
- Client lookup of a Windows service;
- Windows server dynamic registration of a Service;
- Server to Server exchanges of DNS zone information (a *zone transfer*).

Microsoft Windows service resource records are hosted by Microsoft Windows Active Directory servers.

DNS Security is addressed via the use of internal and external name servers (split DNS) and the DNSSEC protocol for updates and zone transfers.

The Internal DNS is deployed as an authoritative master DNS for the POA HNG-X zones. Two servers exist at each POA data centre.

UNCONTROLLED IF PRINTED

FUJ00232658

4.2.1.8 *Intrusion Prevention System (IPS)*

As part of the network security strategy HNG-X is using a McAfee IDS/IPS solution. This solution resides within both the data centres in IRE11 and IRE19, and protects HNG-X infrastructure from potential threats from the WAN i.e. Branch whilst monitoring the traffic traversing between the Core and Access tiers.

The McAfee IDS/IPS 3000 Sensor acts as a security barrier by using both its IDS and IPS capabilities.

- IPS Mode/Policy (In-line) – Used only for Branch traffic monitoring.
- IDS Mode/Policy (In-line) – Used to monitor all other traffic flowing between the Core and Access tiers.

IPS Mode/Policy places the sensor inline and therefore is seen as an active device in the traffic path for Branch traffic and all traffic flowing between the Branch counters and the Core and Access tiers. The traffic is inspected as it arrives on one interface and exits on the other. Any malicious traffic will be denied and an alert sent to the Intrushield Security Manager (ISM) server located in Management Services LAN. Subsequent malicious traffic will be blocked due to the IPS's proactive capability.

IDS Mode/Policy is utilised for remaining flows, and monitors the traffic between the Core and Access tiers by also using in line ports that are connected to the Cisco 6513 Core switches and DMZ firewalls. Any alert notifications is sent to the ISM server in the Core Management LAN.

Sensor Management is via McAfee Intrushield software that is installed on a virtualised Bladeframe server in the Infrastructure Management Domain in IRE11 and IRE19. Access to the sensors for general management, signature and software updates is via this management server. As the software is deployed on a Bladeframe server resilience is provided as part of that architecture. Information can be found within the Platforms and Storage document (ARC/PPS/ARC/0001).

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

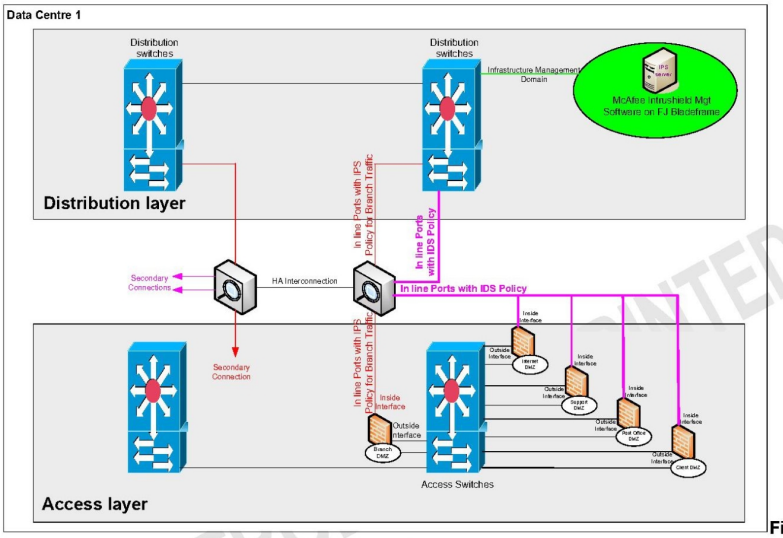


Figure 3

IPS/IDS positioning (logical)

For resilience the sensors at both data centres are deployed in a Failover Pair configuration and must adhere to the following criteria:

Both Intrushield sensors are active at all times. This means that both sensors are ready to process packets on their monitoring ports at all times; neither sensor is inoperative, or in "standby".

Since both sensors see all traffic their state information will be synchronised at all times.

Communication between a failover pair is via a "heartbeat" that occurs once each second. In the event of a sensor failure, and as supported by McAfee's documentation, the expectation of the sensor is as shown in the table below:

Criteria	Expectation
HNG-X Failover Target Time	Expectation is for it to be immediate
Sensor Failover Time	Immediate, as specified by McAfee on Page 2 of Special Topics Guide – Sensor High Availability that "failure is instantaneous and connection state is maintained"
Traffic Loss	None expected , Connection State Maintained as specified by McAfee

Sensor Failover Expectation

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.1.9 *Radius & TACACS+ Services (NRS)*

Network access for branch router and remote support requires authentication, accounting and authorisation. Authentication is providing the 'who you are', accounting is providing the 'what has been performed/audit trail' and authorisation is providing the 'what is permitted to be done'. These are know as the AAA functions and provide the control for key components in the data centre by controlling branch router WAN connectivity and data centre network devices.

The RADIUS protocol is primarily used to provide the Point-to-Point Protocol (PPP) AAA service for branch router WAN access using the various technologies.

The TACACS+ protocol is primarily used to provide the AAA service for branch router support and data centre network access.

The platform for RADIUS authentication (NRS) will use an Active/Active approach with both IRE11 and IRE19 data centres providing RADIUS services. There are no standby RADIUS services at the IRE19 data centre.

The following diagram shows the high-level RADIUS instances and network attachment that will be common for each data centre virtualised server. There will be two RADIUS servers per data centre, following the data centre N+1 strategy.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

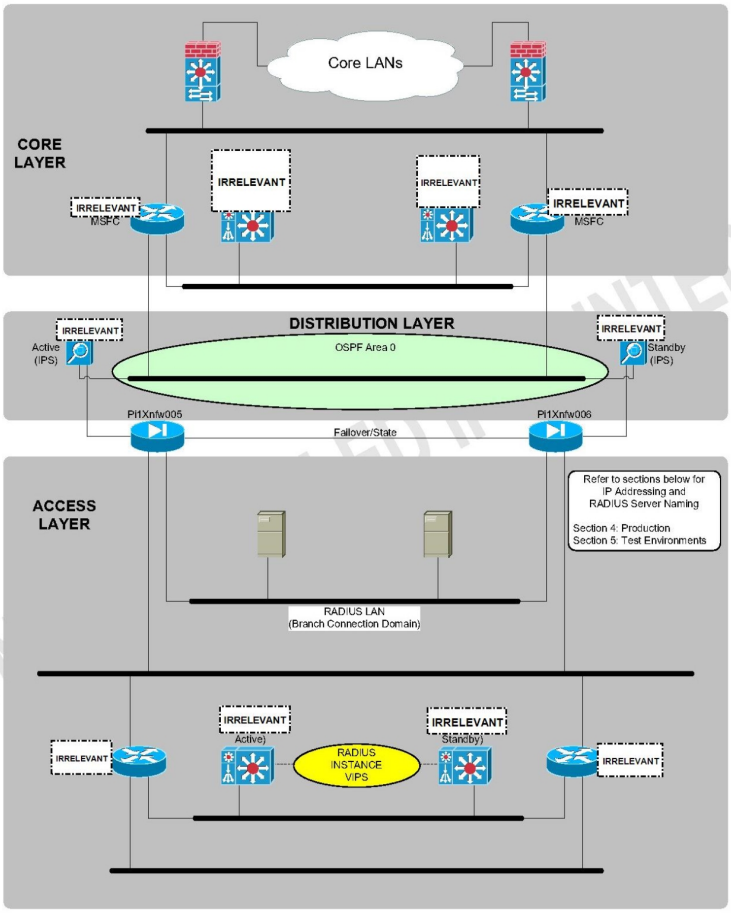


Figure 4

Production RADIUS Layer 3 Network Topology

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.1.10 Key Management Service

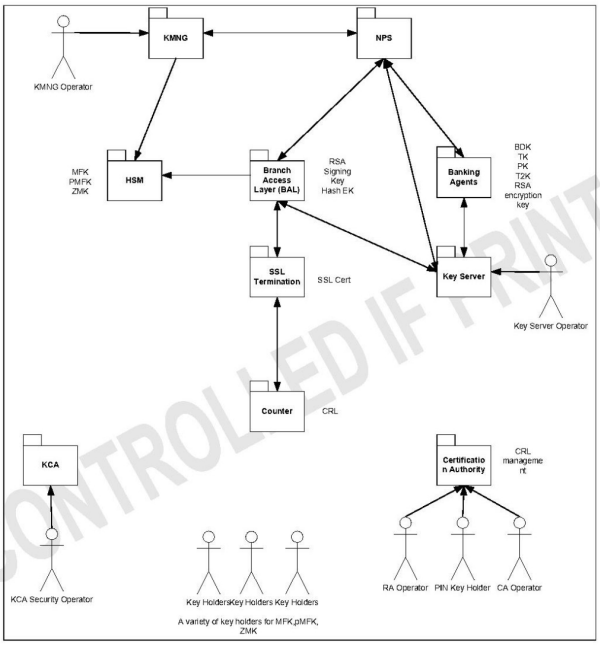


Figure 5

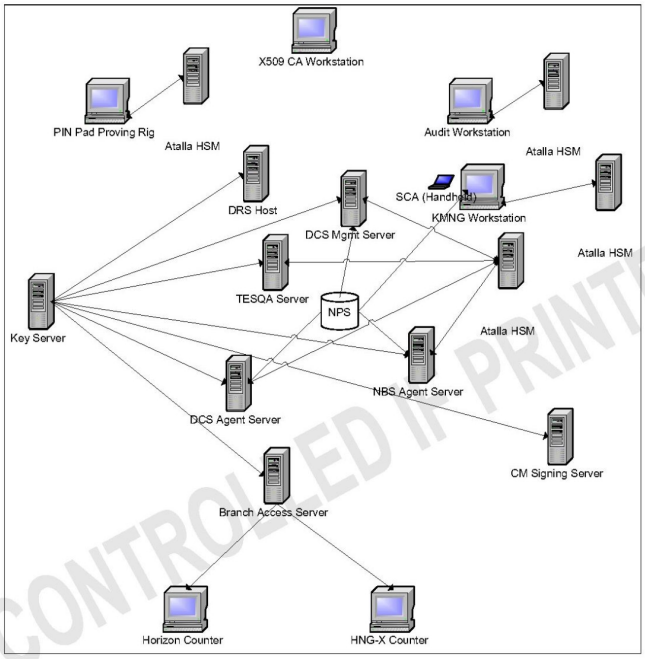
The main components detailed in this design document are shown in Figure 5 above. The roles, responsibilities and key material required by each component are described below.

Note – the diagram only depicts interaction of components as far as key material is concerned, it is not meant to illustrate the run-time interaction of the components.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658



UNCONTROLLED IF PRINTED

Figure 6

Figure 6 gives a more complete picture of new system for HNG-X and old systems that are migrated from Horizon system.

4.2.1.11 Network Persistent Store (NPS)

The NPS is a persistent, fault-tolerant and resilient database deemed to be the repository for sharing key information amongst components. The NPS is the reference point for all key material and components requiring key material must synchronise with the NPS to ensure that correct key material is used.

Further details of the NPS functionality can be found SVM/SDM/PLA/0002.

4.2.1.12 KMNG Workstation

The KMNG workstations provides the user interface for the management of key material. The KMNG provide the following:

Access control to KMNG

Management of MFK and PMFK

Key re-encryption from MFK to PMFK

Management of AZMK

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Management of TK.

Management of PK

Management of T2K

Management of pkcs#12 key sets for other component such as Branch Access Layer, Key Server.

Management of BDK

Management of Money Gram password issued by POA / Money Gram

Management of 192 bit DES key used for protections of CHAP keys

Management of VPN PIN files for BAL and EM

Management of APOP Oracle password.

4.2.1.13 KMNG Operator

The KMNG operator is responsible for the control, management and operations of the KMNG work station. The KMNG operator is two-factor authenticated to the KMNG before any operations are permitted. Two factor authentication depends on the mechanism defined in DES/SEC/HLD/0001.

4.2.1.14 Key Server

The Key Server is responsible for secure distribution of key material to other components within the data centre. Key material distributed generally consists of pass-phrases, and other key material, as required by HNG-X components.

The Key Server runs the KSS application and enables components to access key material stored on the NPS. No component can access the key material from the NPS directly; they must use the KSS to access this material.

The Key Server initialisation is dependant on key material supplied by the sub-Certificate Authority (sub-CA).

The media for distributing the key-set is electronically read from a secure remote management workstation connected to the Key Server.

N.B. A Key Server must always be available for use by HNG-X components requiring key material.

4.2.1.15 Key Server Operator

The Key Server Operator is responsible for providing the initial key information required by the Key Server to complete initialisation, which is strongly authenticated using two-factor authentication, and in addition is responsible for the safe keeping and monitoring of the use of the Key Server key material.

4.2.1.16 Key Server Client

Key Server Client software enables servers requiring key material to communicate with the Key Server to retrieve key material.

4.2.1.17 Key Server Resilience

Resilience of the system is obtained by deployment of 2 Key Servers in the primary data centre.

Resilience of the Key Server service is managed through the Key Server Client that applications use to interface to the Key Server which can detect which Key Server is not being operational at any given time. Whenever a Key Server is detected as being non-operational, an alert is raised which is escalated to Service Management to re-enable/correct the Key Server.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The algorithm used to load balance the Key Server from the Key Client is described in DEV/APP/LLD/0149,

4.2.1.18 Key Server Certificate

KMNG is responsible for storing the Key Server X509 certificate in NPS. The certificate is generated by the sub - Certification Authority. The certificate is presented to the KMNG which reads the relevant data files from the storage media and save it to NPS with the appropriate tag.

The certificate is designated "active" as the current certificate for the Key Server and any previously "active" certificate are designated to "inactive" state.

4.2.1.19 Key Server Access Control

Access to the Key Server workstation is for restricted personnel only. All access must be recorded and the reason for access logged.

4.2.1.20 Key Server RSA Key Set

The Key Server operates under control of an RSA key-set generated by the sub-Certificate Authority and issued in a pass-phrase encrypted file

4.2.1.21 Key Server Initialisation

On initialisation, the Key Server must be presented with the password protecting the Key Server's key-set.

The Key Server remote operator will enter the password and the Key Server will obtain the latest key data from NPS. Using the passphrase, the Key Server un-locks the key data.

4.2.1.22 Remote Management and Recovery

The remote management software is installed and executed on the same platform as the KMNG workstation to avoid the need for a separate platform to host this service.

The recovery process for the Key Server is identical to the initialisation process. The pass-phrase entered by the remote operator must match the currently active Key Server RSA key set.

4.2.1.23 Remote Monitoring

KSS provides a fault tolerant service to components requiring key material. It is essential that the KSS services are always available.

Remote monitoring is required to ensure that the KSS service is always available. If any of the KSS servers are not available, remote monitoring shall inform the security operator to put the servers in an operational state as soon as possible. If there is at least one server operational, it is not essential for the re-started servers to be put into operation state immediately. This operation can be performed outside normal business hours, or during the next day.

In the case of both Key servers being re-started, the security operator must be informed to put one of the KSS servers into an operational state immediately. . The other Key server should be brought into use outside normal business hours, or during the next day.

4.2.1.24 SSL

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- **SSL Termination Point**

  The SSL (Secure Sockets Layer) termination point is responsible for maintaining and terminating SSL encrypted sessions between the Counter and the Branch Access Layer.

- **Other SSL**

  Within the HNG-X solution, there are several clients-server interactions that require the use of SSL encrypted sessions either with server side authentication only or both clients and server authentications.

4.2.1.25 CHAP

CHAP keys are used to establish secure communication channels between branch routers and RADIUS servers at the network level are managed by the Estate Management (EM) component of HNG-X. See DES/SYM/HLD0031.

4.2.1.26 PIN Management

For detailed information refer to DES/MIG/HLD/0006.

4.2.1.27 Counter

The Counters are located in Post Office branches and are responsible for protecting sensitive data exchanges between the branches and the data centre.

4.2.1.28 Hardware Security Module (HSM)

The hardware security modules (HSM) are responsible for providing security services (DES encryption/ decryption, pin block translation) to applications. These devices are networked devices and are accessed by the applications through a set of cryptographic API's.

HSMs are used to carry out the cryptographic functions to protect data that is transmitted from the HNGX security domain to the security domains of the FIs by the Network Banking application and to protect data that is stored within the HNG-X domain both by Network Banking and Retail applications.

Three HPHSMs are installed at IRE11 IRRELEVANT and another two at IRE19 IRRELEVANT.

Two HPHSM IRRELEVANT) shared between LST and SV&I are also located in IRE19. In a DR situation, where IRE11 is lost, IRRELEVANT would be reconfigured for Live use.

4.2.1.29 PIN Pads

PIN Pads are hardware devices attached to the counter.

The cryptographic keys used by the PIN PAD are only used for PIN encipherment.

4.2.1.30 Root Certification Authority (CA)

The Root Certificate Authority is responsible for issuing X509, version 3 certificates. The root CA certificate is distributed, via Configuration Management, to end-points requiring it.

The root CA is only responsible for issuing certificates to other sub-CAs. There is no permanent network connection from the root CA to other systems within the data centre.

4.2.1.31 Secure Configuration Assistant (SCA)

The SCA is used for key generation, key input from paper sources and secure transportation of the key material for processing by KMN workstation. The SCA is responsible for the following keys:

UNCONTROLLED IF PRINTED

FUJ00232658

The SCA device is used to initialise the HSM with the MFK / PMFK keys.

4.2.1.32 Money Gram Password

KMNG is responsible for storing the Money Gram Password in NPS.

Whenever a new password is required, the KMNG will store it in NPS with appropriate key tag to distinguish it from older or current password.

A user interface is provided to allow the operator to activate the password by marking it as “current”.

4.2.1.33 BAL Oracle User Password

KMNG is responsible for storing the BAL Oracle User Password in NPS. A separate password is required for live operation and for training purposes.

The KMNG provides a user interface to generate the BAL Oracle user passwords, encrypting the passwords under a session KEK and storing in NPS with appropriated key tags

Whenever a new password is required, the KMNG will store it in NPS with appropriate key tag to distinguish it from older or current password.

4.2.1.34 Component Interaction

UNCONTROLLED IF PRINTED

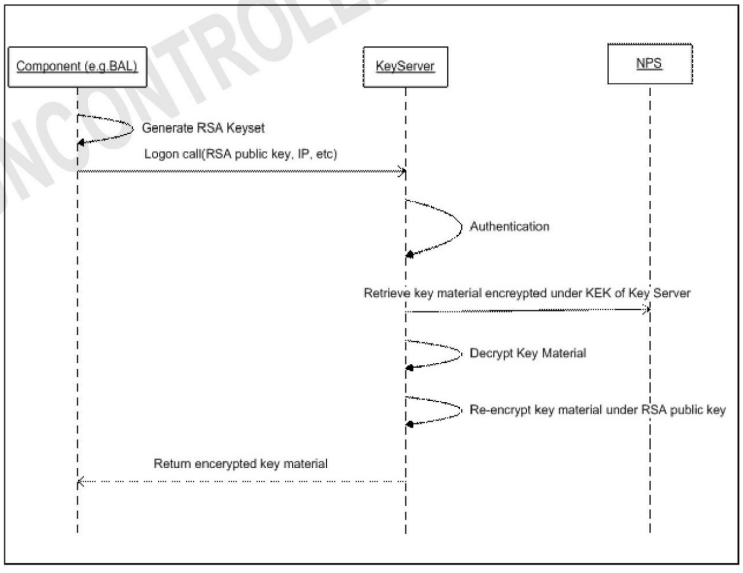


Figure 7

In order to distribute key material securely to components, the component interaction will be as follows:

FUJ00232658

Component generates a temporary RSA key set

Public key sent to Key Server with additional information for identification purposes, e.g. IP address

The Key Server validates the identity of the component

On successful identification, the Key Server retrieved the requested key material from NPS

The Key Server decrypts the key material and re-encrypts them under the public key of the component

The encrypted key material is returned to the component

The component decrypts and recovers the key material in local memory

N.B. The process described above is performed by the Key Server Client which the component interfaces with to retrieve key data from NPS.

4.2.1.35 Branch Access Layer

The BAL signing key is used to sign messages exchanged between the BAL and Counters during the Counter log-on.

On initialisation BAL will interact with the Key Server/Key Server Client to retrieve the pkcs#12 key data and the pass-phrase.

4.2.1.36 Key Enforcement Policy

Key enforcement policy to implement key changes, certificate changes etc will be manually controlled. KMNG is presented with new key material when a new key needs to be put into active state.

4.2.1.37 Key Change Synchronisation

All key changes are manually controlled via KMNG. Any new keys that need to be put into an active state must be done so through the operator options provided by KMNG.

All components requiring key changes must synchronise with NPS via the Key Service/Key Service Client at regular intervals to detect the current active key held in NPS.

4.2.1.38 Identity and Access Management Service

The identity and access management service provides facilities to create, modify and remove users, groups, roles and access permissions. The service controls access at an application and platform level including both local and remote access. This includes access to operational support, system support and data processing systems.

Management in the following list means provisioning, de-provisioning, authenticating and authorising;

1. Operational support users are managed using a directory service for access to Platforms and to Network Devices.
2. Branch business user access is managed using the Branch Database. This includes Global users such as Engineers on site visits and Branch Auditors.
3. Application accounts are managed by the application concerned, except where the application designer has elected to utilise the Identity and Access Management Service.
4. Within the Data Centre, service accounts are managed using the directory service.
5. At the Counter, service accounts are local accounts.

The following facilities are supplied by the Identity and Access Management service. It provides; identification; authentication; authorisation; accounting; non-repudiation; role based access control; and network access control.

- Enables the addition, removal and change of users, groups and roles.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- Enables the addition, removal and change of network systems and devices.
- Enables segregation of duties.
- Controls and enables local and remote access for HNG-X.

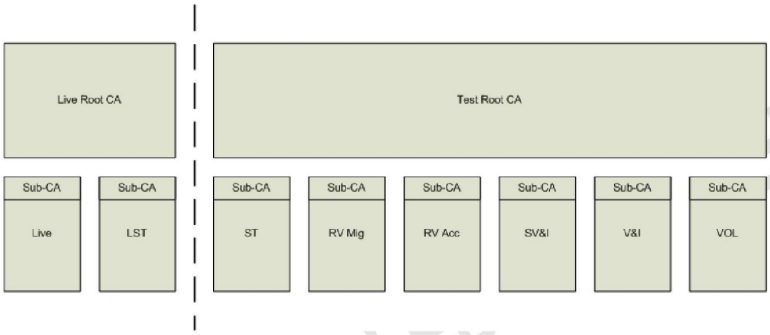


Figure 8

The Live and LST environments share a Root CA as LST is the final testing stage before deployment into the Live environment and therefore it is occasionally necessary to test Live key material prior to use.

Alerts and errors are reported through the event management system.

The public key certificate for the appropriate Root CA and the SSL certificate signing sub-CA will be stored in the Counter certificate store.

Further information is available in these documents;

1. HNG-X Key Management HLD {DES/SEC/HLD/0003} covers the design of the key management system in greater detail.
2. HNG-X Strong Authentication HLD {DES/SEC/HLD/0001} covers the design of the strong two-factor authentication system.
3. HNG-X Crypto Services HLD {DES/SEC/HLD/0002} covers the design of the cryptographic API, (Crypto-API), and key management server, used by Banking authorisation agents, Debit and Credit Card authorisation agents, Audit workstations, Debit Card Management Server, Connect:Direct Gateway Server and the Key Management Workstations.

4.2.1.39 Secure Event Management Service

The secure event management service is a component of the overall Tivoli event management solution, creating events and producing reports using the existing Tivoli event management database. Logs from network devices, intrusion prevention and detection appliances and firewalls are also aggregated by the Tivoli system either directly, or through the syslog server.

Logs are aggregated and analyzed to provide security information and reports. Relevant information will be provided to the CS Security Team through the provision of regular reports.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The following facilities are supplied by the service;

- Provides log aggregation, correlation and analysis.
- Enables security event alerting and reporting.
- Enables compliance reporting with standards and regulation such as ISO 27001 and PCI.
- Enables trending and provides the ability to spot longer term security related events.

4.2.1.40 *Vulnerability Management Service*

The vulnerability management service ensures security patches and updates are maintained at the appropriate level. The service provides secure platform builds that have been hardened to reduce the vulnerability of the standard platform. The service provides protection against malware in the form of Viruses, Trojans, and Worms etc. and detects and prevents malicious code and malicious activity on the network. This service supplies the assurance that possible platform and application vulnerabilities have been reduced to a minimum.

The following facilities are supplied by the service;

- Provides system hardening.
- Provides vulnerability management.
- Provides patch management.
- Provides malware management.
- Controls vulnerabilities within HNG-X.

The vulnerability management service consists of a number of components that work together to identify and reduce vulnerabilities in HNG-X. This includes vulnerabilities caused by configuration errors as well as software bugs.

UNCONTROLLED IF PRINTED

The main purpose of the vulnerability scanner server (VNS) is to detect potential vulnerabilities in the HNG-X environment and report them via the correct mechanism so remediation can be initiated. The server is a Foundstone FS1000 running the database and report manager and resides in the HNG-X Estate and Systems Management Security Domain. All components will be located in IRE11 with a mirrored/replica environment in IRE19 for DR purposes,

The FS1000 has dual processors and a redundant RAID storage system so can withstand a single processor or hard disc failure.

4.2.1.41 *Payment Card Industry Solution (PCI)*

The online system has been designed to ensure that, for online transactions;

- No Debit or Credit card full track information is stored anywhere in the system.
- Banking requires that the full track image is available for up to 5 days, post-authorisation, in the event that a reversal is required.
- No Sensitive Authentication Data is stored post-authorisation for Debit and Credit card transactions.
- As with 1a above, Banking requires that the full track image is available for up to 5 days, post-authorisation, in the event that a reversal is required.
- No PAN (information) is stored in the clear anywhere in the system.

4.2.1.42 *Bluecoat (***Reverse Proxy Service)**

© Copyright Fujitsu Services Limited 2014

FUJ00232658

A new Reverse Proxy Service from Bluecoat® that will be used to control access to the Channel Integration service. A new Network Security layer (Bluecoat) in the Horizon Data Centre to authenticate non Horizon devices before allowing them to connect to HBS

There are security requirements to ensure that only valid devices can connect into the HBS.

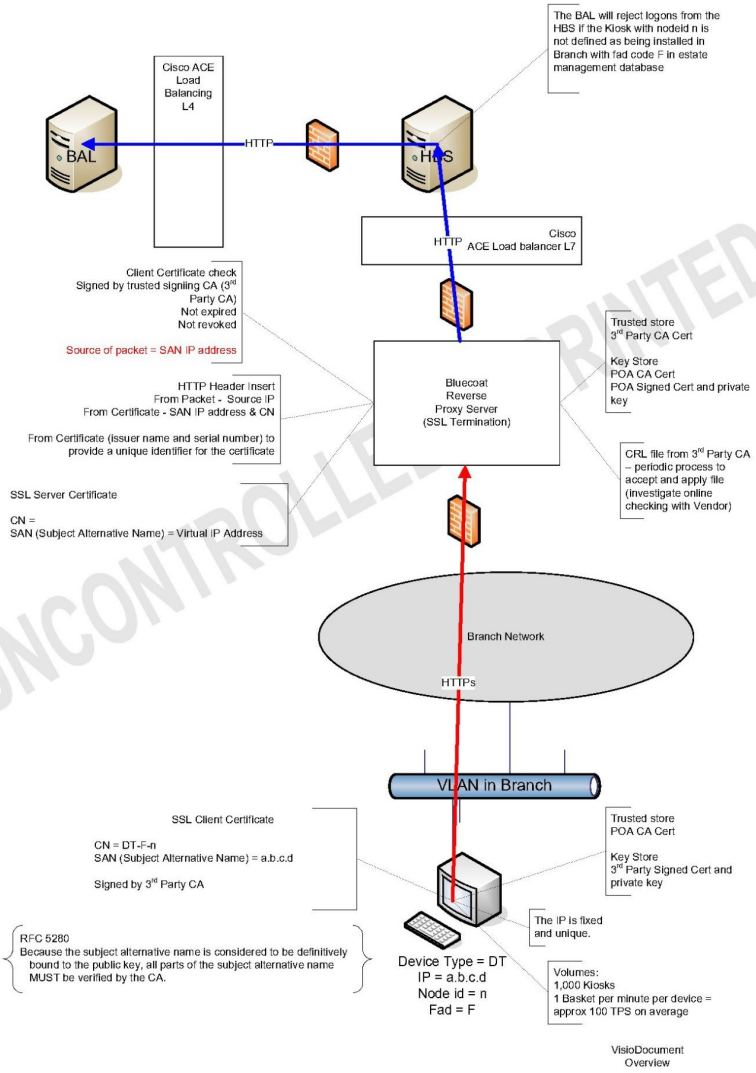
It has been decided that this is something that can be implemented outside the HBS and that it is reasonable to assume that any device that manages to connect through to HBS can be considered to be valid.

The figure below shows the way in which 3rd party devices will connect to HBS and the outline of the security checks that will be enforced.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658



UNCONTROLLED WHEN PRINTED

Security Model for Device Authentication

When the 3rd party device is installed it will need to generate an SSL Client Certificate which follows the following convention:

FUJ00232658

- CN is DT-F-n

  where

  - DT is the Device Type which will have been provided by Post Office Ltd
  - F is the FAD Code (or Branch Code) allocated by Post Office Ltd
  - n is the Node Id which will have been allocated by the Horizon Estate Management System as part of the OBC process

- SAN is IP address

  The IP address will have been allocated by the Horizon Estate Management System as part of the OBC process

It will also need a Public / Private key pair for Payment Authorisation

All of this security material is tied into the logical device, such that if the physical device is swapped, then it needs to be either securely copied to the new device or equivalent security material needs to be generated on the replacement device.

The 3rd party device also needs to know the Virtual IP address of the HBS.

Whenever the 3rd party device wishes to connect to HBS, then this will be done by means of an HTTP Session as described in [REQ/APP/AIS/1794]. This is done by establishing an SSL session to the Bluecoat Reverse Proxy Server, which will intercept connection attempts to the HBS. This means that as far as the 3rd party device the connection is via HTTPS.

The Bluecoat Reverse Proxy Server will then validate the SSL Client Certificate that has been provided and ensure that the source IP address of the connection matches the SAN attribute in the Certificate. It will also add in details from the SSL Client Certificate and a copy of the certificate itself into HTTP headers (having cleared any such HTTP headers if any are already in the message). All other HTTP headers and the payload of the message are passed through.

If all is well, then the Bluecoat Reverse Proxy Server will establish an HTTP connection to the virtual IP address of the ACE Blade that front the HBS and pass through the payload of the original message and the HTTP headers as modified above. The ACE blade then load balances the workload across the available HBS servers, taking into account any "sticky session" routing defined in the HTTP Headers.

When the Message is received by the HBS, then these HTTP headers are examined and the CN attribute is broken down into its constituent parts (ie DT, F and n, using the "-" character as a separator when parsing).

HBS will identify a Device by fields in the ARTSHeader of the messages passed across as part of the Web Service calls to HBS. Specifically:

1. Business Unit: This is the Location of the Device and is expected to be the Branch Code

   This will be validated as being the same as the "F" component of the CN in the HTTP header

2. Business Unit.Name: This is the Organisation that is responsible for the device and is used to control how Cash Settlements are to operate. For Phase 2a, this is expected to always be "POL"
3. Till: This is the Identity of the Device and is used to distinguish between multiple devices at a single location and is expected to be the Node Id

© Copyright Fujitsu Services Limited 2014

FUJ00232658

This will be validated as being the same as the "n" component of the CN in the HTTP header

The Device Type (ie the DT component of the CN in the HTTP header) is then verified as being supported by HBS. A key attribute of the Device type is whether it is manned (ie operated by a clerk) or un-manned (eg a kiosk operated by various members of the public) and this controls how the Log On should be carried out with the OSR. For Phase 2a, the only supported Device Types are unmanned kiosks which use a "User-less" Log On mechanism. This is the only type of Log On supported for Phase 2a. This "User-less" Log On will validate that the Device Type and supplied IP address (ie SAN attribute of the certificate) matches those that have been configured in BRDB for the specified Branch Code and Node ID.

Unless a specific 3rd party device has Logged On, then no other service requests from that 3rd party device are allowed. Therefore it is expected that the first service request in a new HTTP session from a specific 3rd party device is a Log On request.

Manned Devices may require the User of that device to Log On Un-manned devices do not require any further authentication.

Collect & Return - The Collect and Return service is the second of two services intended to make use of the reverse proxy service capability delivered by the Bluecoat Proxy SG appliances

4.2.1.43 HBS- Web Server

HBS (Horizon Business Server) is a platform designed to enable the consumption of services provided by the HNGX infrastructure by applications other than the native HNGX counter.

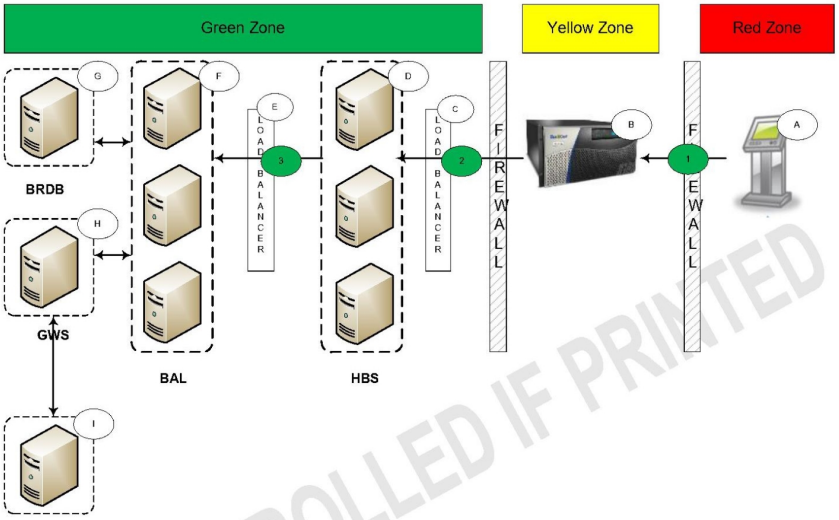
The RTS Web Application which runs on the HBS provides interfaces to consumers to allow the construction of and settling of baskets of transactions. To the 'back-end' HNGX infrastructure the application looks like native HNGX counters, using the same interfaces into the OSR. Note, however, that not all of the interfaces used by the native counters are supported by the RTS Web Application.

The following diagram shows how it fits into the overall architecture.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658



UNCONTROLLED IF PRINTED

The HBS operates as a set of server nodes in a cluster, providing Business Services to a set of terminals in multiple outlets. It uses the services provided by OSR/BAL to fulfil some of these Business Services (and the BAL in turn writes to the BRDB). The Counter business application also connects to the same BRDB instances, but via a different vip for the BAL / OSR.

ID	Component Name	Description and Details
A	KIOSKs	KIOSKs that are connect via VLAN.
B	Blue Coat Reverse Proxy Server	Blue Coat Reverse Proxy Server will ensure that only valid devices get connected to HBS. It provides firewall and HTTPS SSL termination.
C	ACE Blades to HBS	Ace Blades to HBS provide load balancing across multiple HBS farms and nodes in the cluster.
D	Horizon Business Server	
E	ACE Blades to OSR/BAL	Ace Blades to OSR/BAL provide load balancing across the existing 20 live OSR/BALs. If an OSR/BAL node goes down, the current request will fail, but future requests will go to a working node.
F	BAL	OSR/BALs provide the current live service to Horizon counters.
G	Branch Data Base	BRDB provides basket item storage for the estate, and is accessed by other POL and Fujitsu systems to pass on

© Copyright Fujitsu Services Limited 2014

FUJ00232658

		the information to financial, banking and other systems
H	GWS	GWS servers provide access to external third party Web Services
I	Agent	Authorisation Agents for eTopUps etc.

Bluecoat Reverse Proxy Server:

The reverse proxy server checks the certificates held on the consuming devices (kiosks) to confirm their validity.

It is responsible for extracting data from the certificate and inserting it into the HTTP headers forwarded to the HBS. HBS uses this data to identify/confirm the branch and terminal identities in incoming messages.

The principal functions are the NRPs are to terminate SSL traffic (if necessary) entering the data centre, perform certificate revocation checking (if necessary), mutual authentication where appropriate, facilitate anti virus scanning of content of various attributes, according to the specifics of each service

The NRPs implementation and configuration, including the outside and inside proxy VLANs as shown in figure 1, are described in the HNG-X Network Reverse Proxy LLD DEV/INF/LLD2085.

There are multiple applications using the Network Reverse Proxies. The Channel Integration service uses the NRPs, as well as the Collect and Returns service; Smart Metering services (SMS), Common Digital Platform Service (CDP), and HORIce web service.

Channel Integration service is described in HNGX Channel Integration Network LLD DEV/INF/LLD2086.

Smart Metering Service is described in HNGX Smart Metering Network LLD DEV/INF/LLD/2395. HBS is also used as part of the smartmeter service, and initiates an outbound connection to british gas via the DXI forward proxies. Also the smartcard service which involves Ingenico connecting to a VIP presented by the Bluecoats.

Common Digital Platforms is described in HNGx CDP High Level Design DES/APP/HLD/2523

Collect & Return Service is described in HNGx Network High Level Design for the Collect & Return Service DES/NET/HLD/2252.

HORIce web Service- Is used by support teams and the post office to query live and historic data. This design will provide access from the Post Office via the Internet, and from Support location BRA01 to HORIce Web servers via the Network Reverse Proxies implemented in IRE11/19.

UNCONTROLLED IF PRINTED

4.2.2 System Management Service (SMS)

4.2.2.1 Service Summary

The Systems Management Service comprises:

- Event and Systems monitoring
- Software Distribution and Asset Management
- Remote Access and Diagnostics
- Estate Management and Branch Estate Platform Repair

The Enterprise Management software suite (based around IBM TIVOLI software), known as SYSMAN3 is used to support the System Management Service.

FUJ00232658

The Service is based on remote monitoring and resolution which helps to minimise interruptions to the normal business operation of the Branch Infrastructure.

Co-ordination of activities across POA, Support units (Fujitsu and external providers) is provided in order to track changes and resolve incidents, thereby enabling any service degradation to be restore in an effective manner, including any that require multiple Support teams or Service providers to be involved.

4.2.2.2 *Service Availability*

The Systems Management Service is provided by the Systems Management Centre (SMC) and is available 24/7, 365 days per year.

4.2.2.3 *SYSMAN3 Overview*

SYSMAN3 is the HNG-X Enterprise Management solution which manages approximately 30,000 counters (Managed Agents) in Post Office Outlets and another 250 Data centre Campus based Servers.

The products include applications which provide access for both users and administrators; some of these applications are accessed via web browsers such as Internet Explorer, whereas others provide specific desktop applications using technology such as Java.

Access to all SYSMAN3 applications will be via the SSN (Secure Access Server) platforms. These are dedicated Windows 2003 servers running Terminal Services which provide secure access to all of the data centre platforms. All users who require access to SYSMAN3 applications will need to connect to the appropriate SSN platform and logon using their Active Directory username and password.

4.2.2.4 *Tivoli Management Framework (SYSMAN)*

Management comprises 3 key components; Active monitoring with IBM Tivoli Monitoring, Event alerting with Tivoli Netcool, Software Distribution with Tivoli Provisioning Manager and and Software Distribution with TEM (Tivoli Endpoint Manager) to the counter estate.

The environment can be split into several layers.

Agent level – agents exist on Servers and Counters, either the initial receptor of a system fault or the target for data distribution or a system request.

Comms level – Server processes that provide distributed services to higher level management services and load balancing gateway communications between agents and applications. (e.g. EFS)

Collection level – Focal point processes for Monitoring and Event data (e.g. EMM, EES)

Management level – Services providing User Authentication, Storage of Monitoring and Event Data, Administration, Business Process triggers and execution of Software Provisioning (e.g. EMS, EPM, EDS & TEM)

User Level – Top level Data Reporting facilities and browser based views of Events and System status. (e.g. EMD, EUI, EAS, ERP)

4.2.2.5 *System Management Platforms*

The platforms required to support monitoring may not be dedicated to a single function, but may also host other software functions within the System Management architecture.

UNCONTROLLED IF PRINTED

FUJ00232658

The software applications to be hosted on the platforms are shown below:

Platform Name	
EMM	System Enterprise Monitoring Server
EUI	System Enterprise User Interface Server
EMD	System Enterprise Monitoring Display
EES	System Enterprise Event Server
EAS	System Availability Server
EFS	System Enterprise Fan-out Server
EDS	System Enterprise Database Server
TEM	Tivoli Endpoint Manager

The EMM and EUI platform instances together form the ITM environment.

The EED, EMD and EFS platform instances will provide the Object Server layers and Proxies for the Tivoli Omnibus event solution.

The EAS platform instances provide the Business Service views Real Time Active Dashboard (RAD).

The EDS platform instance provides the Oracle RDBMS for the SYSMAN solution.

The TEM platform instance provides the software distribution to the counter estate.

UNCONTROLLED IF PRINTED

4.2.2.6 Event & Systems Monitoring

The Systems Management Service provides event and systems monitoring of both the Branch Infrastructure and HNG-X Central Infrastructure. Events are the indications of conditions that have operational significance to either the Branch Infrastructure or the HNG-X Central Infrastructure. They include Software, Hardware or security conditions that may require investigation and also include occurrences of particular, repeated events, for example, a low battery in PIN Pads. Investigations will involve either other relevant Operational Services or a defined recovery procedure.

Operational platforms have performance monitoring Software installed and this is available to the Systems Management Service to enable systems monitoring to take place.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The following diagram highlights the location of the agents, the Campus Server agents are also installed on all SYSMAN3 platforms.

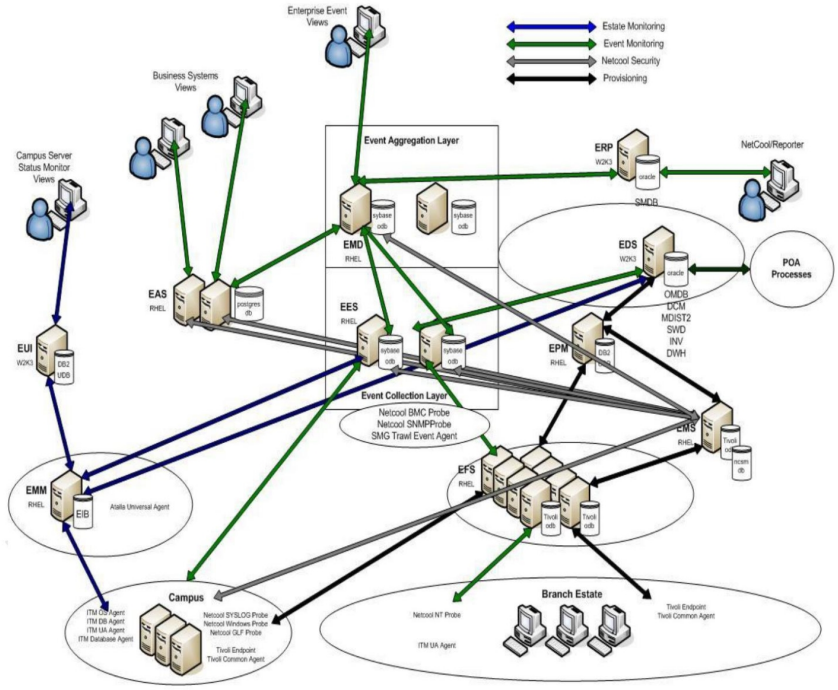


Figure 9

4.2.2.7 Fujitsu Network Management Systems (NMS / NNM)

HP OpenView, Cisco Works and a number of diagnostic probes are located in each Data Centre.

The NMS also monitors the Branch network via the Branch router. The network is treated for management purposes as entirely Production, with isolated areas of testing. This is to ensure that the secondary site network is always ready to act as the DR target.

HP OpenView gathers SNMP events from network equipment, filters the events, and forwards them to Tivoli (SYSMAN). OpenView also actively probes for managed devices, such as servers, and raises an alert if the server cannot be contacted.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The NMS is accessible by different teams, including the SMC (India), the Network Support team (Warington) therefore in the event of a connectivity problem by any one team then monitoring is still possible.

The Network Management System comprises a set of software applications hosted on various platforms and appliances. They are shown below:

Platform Type	Description	Software Application	Platform Operating System
NMN	HP Open View	HP Network Node Manager	Solaris 10
NCW	Cisco Works	LAN Management Solution	Solaris 10
NFM	Cisco Security Manager	Cisco Security Manager	Windows 2003
	Cisco Fabric Manager	Cisco Fabric Manager	
NPC (Appliance)	Probe	Wireshark	Windows 2003
SYS	Syslog Server	Syslog-NG	Red Hat Enterprise Linux

UNCONTROLLED IF PRINTED

4.2.2.8 *Real Time Active Dashboard (RAD)*

The Tivoli Netcool Real time Active Dashboard (RAD) is used to provide a real time GUI view of the HNG-X Business Processes, primarily used by the SMC during systems monitoring. In addition information is available for the Service Desk, Service Management and the SSC.

The Business Service Views are intended to give a high level indication only of the status of all of the HNG-X Services using a selected subset of the events produced by those Services. Low level detailed event information will be maintained by the various Component Management Systems and also can be accessed either by the Netcool AEL (Active Event List) or via Tivoli Reporting tools against the ERP.

4.2.2.9 *Software Distribution and Asset Management*

TPM 5.1 supports software distribution using two separate methods, Framework and workflow based. The Framework based distribution is updated from the earlier versions of TCM, both methods will be used within SYSMAN3 for 'Horizon Online'. The workflow method is a TPM facility to allow single or low concurrency actions and will be used for immediate updates and Branch Router updates.

In all cases the package that is delivered will have been pre-prepared to allow a number of functions; whatever occurs in the distribution and installation scripts is not directly a property of the underlying infrastructure.TEM supports distribution and installation via its Relay structure to ensure single delivery over slow links. The fixlet that defines the installation applies the fix when it is relevant (time, product dependencies etc.).

TEM based distribution:-

Tivoli Endpoint Manager's architecture for software distribution, uses a single Central Server (TEM Server) connected via a hierarchy of TEM Relays to endpoints running the TEM Client; the Relays ensure that packages for distribution only make a single traverse of the path between any two relays. The positioning of the Relays can be automatic, using network query to find the best route, but in the solution for 'Horizon

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Online' the relays will be pre-determined and configured manually to ensure best fit for the unusual demands of the estate.
The only software distribution method available in TEM is a 'PULL' paradigm where the TEM Client is informed of potential actions and pulls the software through the Relay structure. An apparent 'PUSH' paradigm is achieved by the TEM server sending out a UDP prod to every target involved when a distribution action is taken in the TEM Server; the receipt of this prod causing the Client to evaluate and update software as relevant.
The TEM architecture will conform to the 'Horizon Online' architecture with TEM server and the TEM relays being in the 'active' Campus. Fallback for failing servers is on a plus one basis, with defined DR being achieved by moving the compete solution to the alternative Campus. However, TEM relays will be configured with primary, secondary and tertiary routes, ensuring alternative paths during most 'single point' failure scenarios.

At the endpoint, the TEM Client must be installed. The TEM Client together with the related central service provides authentication, secure communication and endpoint operations. TEM Relays may be activated on any TEM Client, so within the Branch estate Relays will be defined in some of the Branch Counters. The TEM Client runs continually within every endpoint and ensures conformance to policy while collecting change data which is relayed back to the TEM Server The TEM Client also performs operations on behalf of TEM server, providing its functionality through 'fixlets', 'policy' and 'tasks'.
The term 'fixlet' defines a set of steps that are taken each time the fixlet is inspected. These steps include inspection for the relevance of the fixlet and actions that must be taken to correct the situation. Once the situation is corrected the fixlet is no longer inspected. This is usually associated with the delivery and installation of software updates.
The term 'policy' defines a similar concept to the fixlet, but the policy is continually inspected even after corrective actions have been taken. This is usually associated with actions taken to ensure ongoing compliance with a standard. The term 'task' is similar in concept to the 'fixlet', but associated with actions to be taken on single, or groups, of endpoints rather than globally. An example may be to start a service on a single counter.
The TEM server includes a database instance that records all actions and endpoint acquired data. All managed endpoints run the TEM client and configured endpoints also run the TEM Relay. All software to be installed is held in a private cache within the Relays as a SHA1 file; at installation time it is transferred, unpacked and validated into the Client cache from where any installation process is run by the Client. Packages will be received from Configuration Management into the NAS interface; TEM policy will pick up the new packages and introduce them and associated default fixlets to the TEM Server. Actions taken in response to Release Management instructions will ensure that the packages are delivered to relevant TEM Relays and subsequently installed.

TEM Relays are configurable to allow bandwidth control and toonly take actions in relevant time windows.

Workflow based Distribution and installation:-

TPM supports workflows, which are essentially scripts or programs that run under TPM control but with interface to the TPM Data Model.

The TPM Data Model is a database schema supported on a Database server; this records all software distribution actions taken by TPM as well as holding a software inventory of all deliveries via TPM.

Standard workflows are provided with TPM and new ones can be easily added.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Workflows will exist to install packages in rpm and msi format, and also in SPB format; this means that the standard software packages released from configuration management can be distributed and installed by workflow.

The user will simply use the TPM GUI to make the requests which are added to an activity queue within the data model; the relevant workflow will process these request.

This form of distribution will be used for 'one-shot' updates. It will also form the basis of Branch Router update since it is the only facility that can work in an endpoint agent free environment.

The infrastructure that supports this form of activity is the TPM server with its Database and a method of authentication on the target device (TCA for platforms, telnet, ssh, scp etc. for agent free). It should be noted that the TCA is only installed in HNG-X compliant Campus Platforms and that the agent free methods are only supported within the Branch Router. This means that workflow based distribution is only available to Campus Platforms (excluding those running Windows NT or Solaris 8) and Branch

Routers.

The following will be required for PUSH or PULL distributions:

A method for targeting a Specific software package at any portion of the managed estate, to include:

- pilot distributions
- subset of targets based on branch specific criteria e.g. number of counters, location. Etc.
- subset of targets based on network considerations e.g. Satellite only
- control of targets based on the software inventory
- Control of targets based on general database queries, where the node name is a property or linked property of the database tables queried.
- whole estate

Other controls include:

- Maximum retries
- Priority control
- Specified timed windows, to include distribution only, installation only, both, no use.
- Knowledge of how long an action takes to ensure window closures are not overrun
- Cancellation of PUSH distributions, which should stop at the earliest possible moment. It will not be possible to stop an installation that has already started.
- Control Maximum network usage from any Relay.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

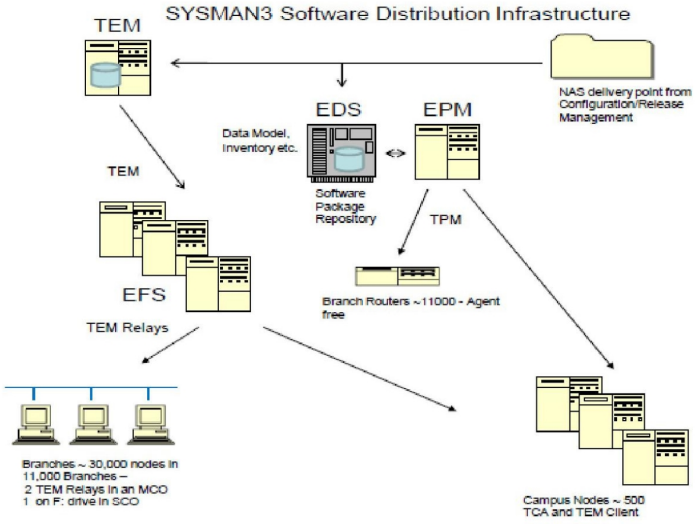


Figure 10

Software Distribution Infrastructure

4.2.2.10 Remote Access and Diagnostics

All support staff connect to Secure Access Servers (SAS) resident in the data centre using workstations at a defined software level as the only point of access. The connectivity may be from Corporate LAN or from an extension of the Campus LAN. In the Corporate LAN case a Corporate build workstation with a fixed IP and secure certificate will be used. In the extension Campus LAN case a formal POA workstation build is required.

The connect route may be from Fujitsu sites or Out of Hours from home locations. There will be specific challenges en route depending on the locale of the workstation.

At the SAS the user will be authenticated according to the Identity Management System that incorporates 2 factor authentication and results in the user being legitimised to operate in a defined role

The SAS provides onward access to data centre platforms and the branch estate using 3 rd party COTS product management interfaces and audited client access via proxies (for example SSH client or System management Tivoli).

When accessing the platforms then the role of the calling user is used to determine access to the Operating system, file systems, databases and applications.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

There are three SSN Servers in each data centre to provide resilience (six in total).

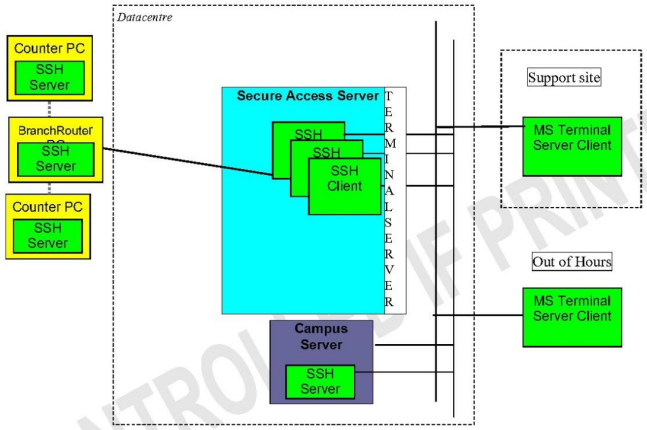


Figure 11

Overall infrastructure showing onward access via SSH

UNCONTROLLED IF PRINTED

Onward access into the System Management framework provides its own role paradigm that mediates access to Tivoli objects and functionality. The Tivoli functionality covers all facets of software distribution, monitoring and tasks.

As well as traditional Framework based tasks there is also workflow tasks available through TPM; these allow agent-less access to the Branch Router as well as agent based access to other platforms.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Figure 12 – System Management framework solution below illustrates the TPM workflow access entered off the SSN Server, via the EPM, which passes through the management platform to reach the server, counter or branch router that is the target of the management operation.

The system management framework is discussed in detail in ARC/SYM/ARC/0004.

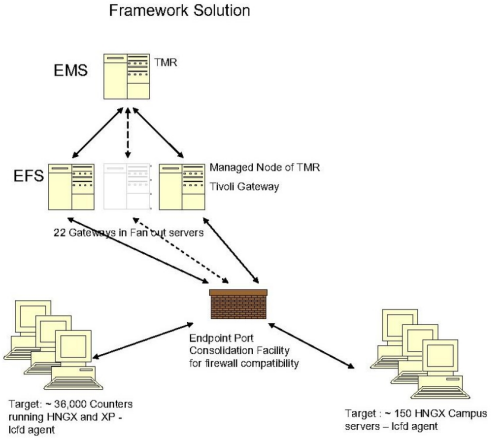


Figure 12

System Management framework solution

UNCONTROLLED

FUJ00232658

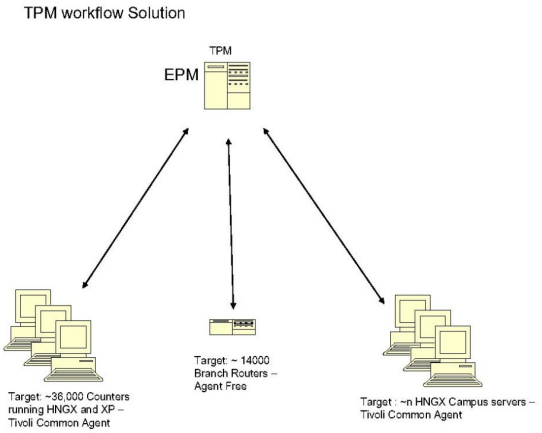


Figure 13 – TPM workflow access solution

4.2.2.11 Time Synchronisation

The first stratum is the primary time source, being a highly reliable GPS (Global Positioning System) satellite network. A data centre resident GPS time server uses rooftop antenna to receive signals from the satellite.

The secondary stratum is the data centre which contains all the server platforms and network appliances.

These platforms poll the primary time server and request the time in UTC (Coordinated Universal Time) format. The NTP (Network Time Protocol) product on the platform is configured to achieve millisecond accuracy but will also protect against large clock shifts in a single request after the first synchronisation on reboot.

If the GPS primary time server is not available then the server automatically switches to an alternative primary time server.

If the alterative GPS primary time server is also not available then the server uses another server in the stratum as the primary time source.

The third stratum includes all Active Directory Clients including subdirectory controllers. The subdirectory controllers act as time sources for all of their Windows based clients and will technically be stratum 2+. All Windows based workstations, irrespective of physical location, will be served by the Active Directory Domain to which they belong.

The fourth stratum is the branch estate and any servers on client site's that are owned and managed as part of the HNG solution. For example the latter class includes file transfer platforms.

The branch estate uses NTP to synchronise with one of a set of nominated servers within the data centre. The period of polling and the selection of server for a branch will be based on an algorithm such that each counter can keep their clock accuracy within seconds, with a defined level of network quality of service.

The servers on clients' sites use the same architectural solution as the branch estate. The polling interval though may well be constrained by the nature of the network connection to the data centre. For example, it may be a dial-up connection which is charged per connection.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Any time-synchronisation request in the estate that results in a clock change will generate an event message that is forwarded to the data centre and into the long term audit. Clock changes in the data centre are also be audited. The audit provides ancillary evidence to fraud enquiries where the transactions have been logged with the local clock value.

•

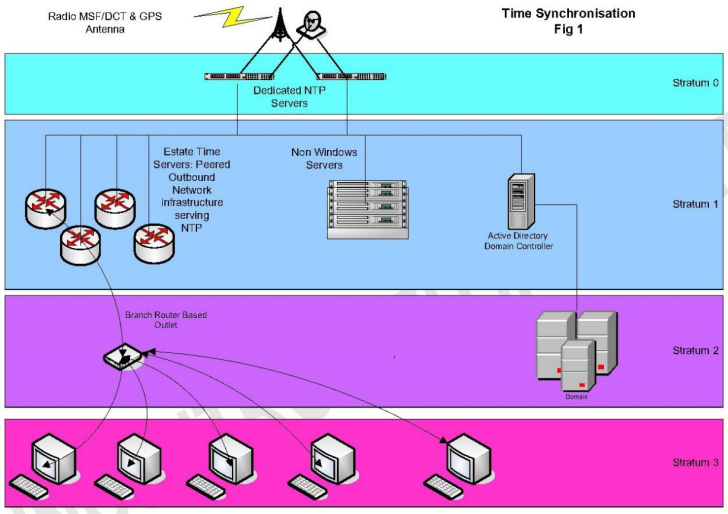


Figure 14

Time synchronisation infrastructure

Details of the time synchronisation solution will be found in the following document: DES/NET/HLD/0013

4.2.2.12 High Level Scheduling

The TWS scheduling product provides an enterprise level functionality derived from the Horizon Maestro solution:

.

All access to the scheduling system is role based and that role definition shall include capability to restrict functions by role (e.g. a monitoring role that has no change capability).

Details of the scheduling solution can be found in DES/SYM/HLD/0016 and DES/SYM/HLD/0025

4.2.2.13 Enterprise Boot Server (EBS)

The EBS (Enterprise Boot Server) currently provides a "bootstrapping" facility to enable the automated installation of operating systems onto the target hardware. It does this by providing Jumpstart

© Copyright Fujitsu Services Limited 2014

FUJ00232658

capabilities for Solaris deployment, NFS shares for Linux kickstart deployment and Samba shares for Windows unattended deployment. It also runs scripts to generate the platform configurations. The EBS function will now be provided by the BSS and BSL servers since the current EBS is currently being shared across rigs, which is a security risk. EBS has also not got sufficient capacity to enable the provision of newer versions of Operating Systems. The removal of the EBS server will also reduce the hosting and support costs.

To overcome the issues the existing BSS (Solaris Backup Service) will be used to provide the required jumpstart service and the solaris media files used during the jumpstart process. The BSL (Linux Backup Service) will be used to provide the NFS shares required for the Red Hat builds and SAMBA shares for the Windows builds.

Resilience for the LIVE boot servers is provided already since there are already two BSS and two BSL servers in LIVE, one in IRE11 and one in IRE19 which provides redundancy in case of any failures at either site. There will also be a share, BFDR, created from BSL1 and BSL2 (Production only) and the Bladeframes will dump to BSL1 and BSL2 /export/pan_failover

This area will be committed to tape as part of the standard BSL backup which is currently not possible in the existing environment.

There will be no redundancy for the SV&I and LST environments.

Bladeframe PAN Manager functionality is also used to aid platform foundation provisioning within the Bladeframe.

The platform foundations are deployed by running scripts on the BSS and BSL servers and PAN Manager (for servers located on the Bladeframe). These scripts are called by the Tivoli Provisioning Manager

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

System state after yet to be defined CP0808 still using Tactical DXT

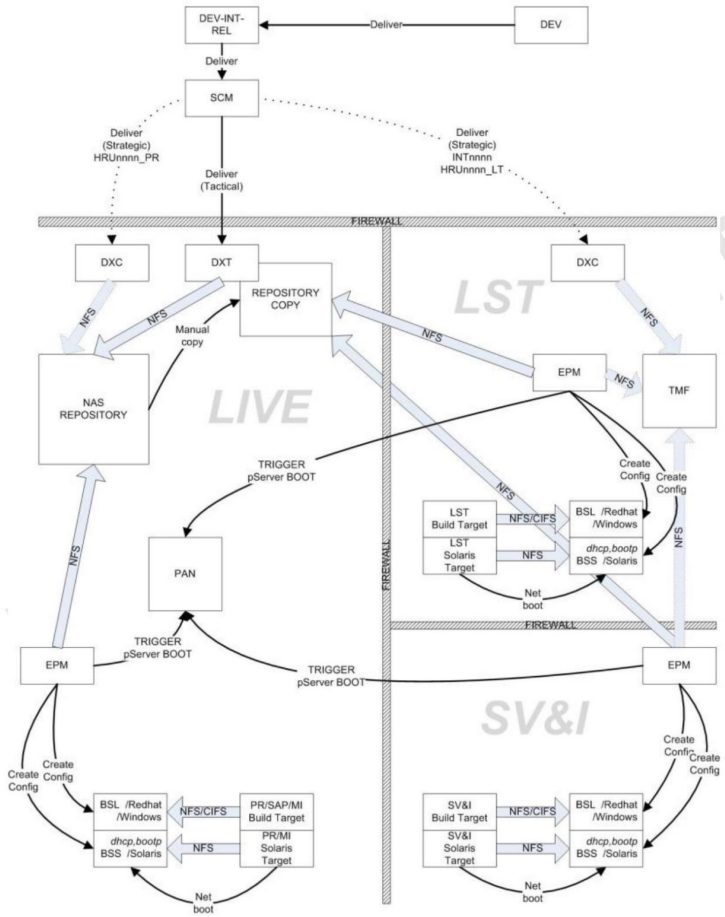


Figure 15 Bootstrap Process

4.2.2.14 Server Provisioning

The Tivoli Provisioning Manager (TPM) product is used in building platforms from the base hardware when it can provide facilities to equip a native hardware platform with an operating system image, personalise the image, and then layer middleware and application packages using the same software distribution technology and packaging as incremental updates to a live platform.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

It should be noted that within the Bladeframe the native build from image may utilise Bladeframe PAN Manager scripts rather than build from image.

The delivery results are stored in a persistent inventory and reports or displays are available through the standard product, and customised reports can be generated.

4.2.2.15 Service Monitoring

This is performed by event flow; events may be collected in both an active and passive manner, and alerts may be created by sampling, aggregating, correlating or apply other rules on the raw incoming events. The Tivoli Netcool RAD (Real Time Active Dashboard) product, which uses a GUI interface, is configured with the business rules required to map such events into business services, and samples the event and alert flow to display the required information,

The services monitored in this way include services offered by SYSMAN3 itself (e.g. software distribution, event flow etc.) as well as mapping business applications (e.g. NBX, DVLA etc.)

4.2.2.15.1 Active Monitoring

Active monitoring is achieved by agents looking for known stimuli and raising events via the relevant Event Logs. This may take the form of in-built functions (e.g. processor utilisation > 80%, service X not running) or bespoke applications (e.g. script to confirm connection to URL).

In some cases the event flow may be through ITM to the managing system, where it will then be directed into the main event flow.

Active monitoring is available in the branch estate via the ITM Universal Agent. Active monitoring is available in the campus estate via the ITM Universal Agent and the ITM Operating System Agent. These are supported by a full ITM structure (TEMS and TEPS). Other agents are also employed for specialised monitoring (e.g., Oracle database).

The IBM Tivoli Monitoring (ITM) suite of programs will be used for active monitoring.

4.2.2.15.2 Passive Monitoring

Passive monitoring is the process of collecting events that are already created within the environment (e.g. in the UNIX Syslog or Windows Event Log etc.). Such events may then be analysed and forwarded to a central repository as required.

The events may be categorised, aggregated and potentially correlated at the event source; by this means it is possible for events to contain a varying criticality status. It is also possible to detect duplication and excessive flow from a particular source and perform flow control and/or event replacement.

4.2.2.15.3 Event Processing

The events selected, after the rules are applied at the source, are forwarded through the network infrastructure to an event collection layer which are defined as an event sink. The others will remain in the underlying source but are not forwarded.

When circumstances are such that the Tivoli event probe cannot forward the event (e.g. Network failure etc.) the events will be cached and forwarded later.

Within the event sink it is possible to carry out further aggregation, de-duplication and correlation of events received from different sources. By providing a single sink it is possible for all current events to be in context at the same time. This allows alerts to be created from events.

The events received at the sink are passed into an Oracle database to allow for an event audit trail, statistical analysis and historical event searching over a controlled period

The events received in the sink are optionally forwarded to two separate display layers:

UNCONTROLLED IF PRINTED

FUJ00232658

An event viewer where, any event of sufficient criticality may be viewed.

A business service monitor, where combination of events and alarms are configured to display the health of each business service.

Using the above it is possible for support staff to see the underlying cause of problems and also to be alerted to problems that are affecting the service.

For example it may be possible that the loss of a single server will not stop any business service, but will either affect its performance or resilience; in such a case the combination of service monitoring and an event viewer allows support staff to be alerted and to take the necessary corrective actions.

It should be noted that such monitoring action does not rely on the events held in the Oracle Database.

4.2.2.16 Branch Agent

The ITM agent that is used within the branch estate is the Universal Agent.

The HNG-X Branch solution is configure to send data to the data centre this will be achieved by writing to the NT Event Log to allow data to be forwarded via passive event monitoring.

This solution allows monitoring and optional restarting of services in the branch estate with events returning via the event management infrastructure.

4.2.2.17 Campus Agents

In the Campus both the Universal Agent (UA) and the Operating System (OS) agent are deployed.

A full Tivoli Enterprise Management and Tivoli Enterprise Portal infrastructure are deployed as illustrated in the following diagram, where the TEMS layer receives events from the agents and the TEPS layer is responsible for correlation and display

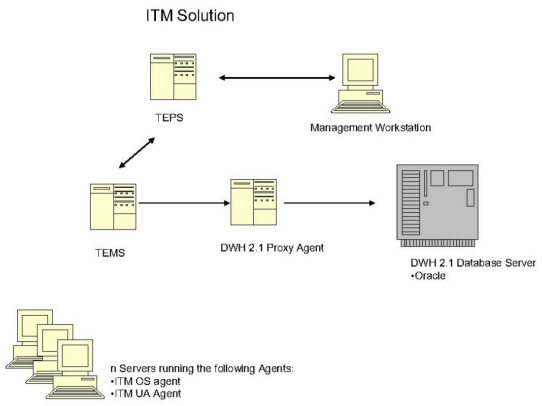


Figure 16

ITM Solution

UNCONTROLLED IF PRINTED

FUJ00232658

It should be noted that the Data Warehouse mentioned above is an internal function of the ITM software.

4.2.2.18 Related Actions

ITM allows series of events or stimuli to be defined as 'situations'. It is possible for the structure to take actions based on events received and the defined 'situations'.

4.2.2.19 Event Management Infrastructure

This is based on the Tivoli Omnibus suite of products. The event collecting agent is referred to as a Probe and all Probes are configured in 'store and forward' mode to ensure reliable event delivery.

4.2.2.20 Branch Counter

Within the branch estate events are collected via the Windows Event Log. All applications write exceptions and potentially positive information to the log; a Tivoli NT Event Probe receives all events from the Windows Event Logs and pass them through a rule set to decide on forwarding. The Probe is compatible with both Windows NT and XP.

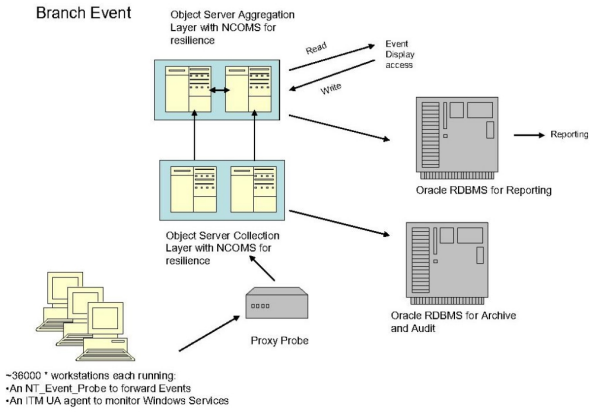


Figure 17

Event Management Infrastructure – Branch

With reference to the illustration above:

There is enough Proxy Probes to ensure that no Proxy Probe has more than the maximum supported number of Tivoli NT Probes sending events to it

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The collection layer accepts all events from all Proxy Probes and writes them to the Oracle database as an historical archive.

The collection layer and its Oracle database write all received events to serial files as an audit trail and allow searches on raw events received.

A subset of events, those requiring the attention of support groups are passed to the aggregation layer.

Both a web and console access is offered to view these events, access to the relevant option being user and role based.

Event updates from the consoles are written back to the aggregation layer, to ensure that event data is coherent for the user but not re-written to the audit and archive databases.

4.2.2.21 Branch Router Events

HNG-X branches have a Branch router to control communications.

The router can forward data, which can be seen as events, in two ways:

1. Local Events – Syslog messages from the router are directed on the local branch LAN and are picked up by a CNIM process in one of the counters in the branch; this process writes events to a local log file and any events it considers for forwarding to the NT Event Log.
2. Remote Events – Syslog messages from the router will be directed over the Wan to be picked up by the relevant Network Management system.

As well as simply forwarding events received from the router, the CNIM activity also processes the events it receives to determine Quality of Service metrics and generates its own events, to inform of changes in base communications etc.,,

Other events pertaining to the Branch router are received from the Estate Management Boot Platform, which is a Campus Platform. This platform is responsible for initial provisioning of the Branch router and forwards information about initial provisioning, registration and inventory, as events.

It should be noted that certain events from the Branch router, via NT Event Log, or the Boot Platform have significance that must be interpreted by rules in the event receiver, and relevant actions taken.

An example of this is during Branch Router provisioning when events are sent from the Boot Platform via the Microsoft Event Log. These events contains details of the Branch Router including its name, Branch Code, Serial Number, interface serial numbers, GSM PID, QOS etc. ; Event rules are applied to add the Branch Router managed object to the TPM Data Model and to update its inventory with the specific data.

4.2.2.22 Campus Events

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

As well as an event flow like the branch estate the campus also receives events from sources such as ITM, SNMP, text files etc.

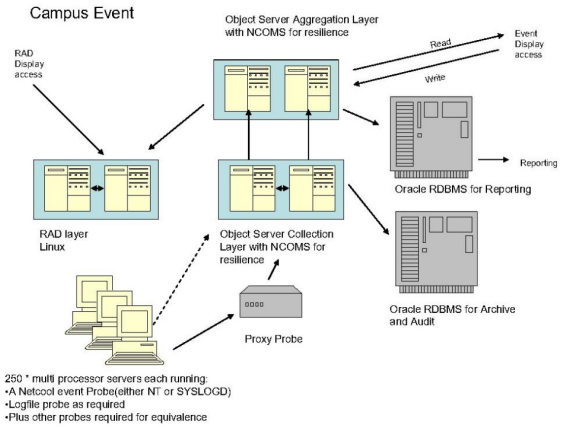


Figure 18

Event Management Infrastructure – Campus

With reference to the illustration above:

Probes may talk direct to the Object Server collection layer or via a Proxy Probe; this will be configured to ensure that the Object Server does not exceed its maximum connection limit

Although Campus Platforms are shown as directly connected to the Object Server, a Proxy Probe may be introduced if the number of Platforms threatens to exceed the Object Server connection limit.

A number of Probes are used to accept events from sources such as SNMP, Oracle, Sysco, text files, Windows Event Logs etc.

The collection layer accepts all events from Proxy Probes and Probes and writes them to the Oracle database as an historical archive.

The collection layer and its Oracle database writes all received events to serial files as an audit trail and allow raw event searches by SQL query if required.

A subset of events, being those requiring the attention of support groups, are passed to the aggregation layer.

The aggregation layer and its Oracle database offer a reporting interface on significant events.

Event updates from the consoles are written back to the aggregation layer, to ensure that event data is coherent for the user but not re-written to the audit and archive databases.

Business system views are provided by the RAD layer. Its rules are configured to access the events by query into the aggregation layer, providing service and component views.

The structure above allows the receipt of Campus events from any event raising source.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.2.23 Links to Known Error Logs (KELs)

Certain events may already have been considered and known error log entries may have been raised to describe the cause and possible remedy for such an event. Mechanisms are provided to display, on request, any known error log entries for a particular event or alert; these, by their nature, are requested processes.

4.2.2.24 Related Actions

Rules are applied to events for correlation and/or aggregation in collection and aggregation layers. As well as altering the state of events or raising alerts from events the rules can call external programs or scripts to allow reaction to events.

4.2.3 Operational Business Branch Change (includes OBC) Management / Estate Management Service

4.2.3.1 Branch Change Management (includes OBC) Overview

Branch Change Management changes are delivered to the OBC Team (Outlet Business Change - based in Crewe CRE02) from the Post Office, and by Customer Services in response to changing Network Service costs. OBC operations are implemented in the Branch Change Management System (BCMS).

Changes are to the physical branch estate and include such requests as:

(a) Branch closures;

(b) Branch openings;

(c) Branch re-locations;

(d) Branch refurbishment;

(e) Counter Position increases;

(f) Counter Position reductions;

(g) Branch conversions;

(h) CPU relocations;

(i) Exchange of fixed Counter Positions with Portables and vice versa;

(j) ADSL porting service;

(k) Emergency re-openings; and

(l) POMS installation and removal

The overall workflow of an OBC change can be summarised as follows:

To acknowledge and enter the OBC change into a scheduling system. To provide requests to any necessary external parties to provision the OBC change. To schedule the timely update of any Data Centre application's configurations that are impacted by the OBC change (this may for example require adding or removing Branch Authentication data). The timely and automatic provision of any new or changed

UNCONTROLLED IF PRINTED

FUJ00232658

personalisation data for the Branch router and/or counter affected by this OBC. The automatic installation of the personalisation data at the time of any physical installation of the counter and/or Branch router associated with this OBC. The provision of invoicing to Post Office. The ability to report on the progress and/or change an existing OBC schedule in accordance with agreed policy.

- The update of central configuration repository such that the support staff always have an accurate view of the status of a Branch.
- To respond to and action (where feasible) amendments to the OBC request by Post Office.

For more information see OBC Branch Change Service (SVM/SDM/SD/0014).

UNCONTROLLED IF PRINTED

4.2.3.2 *Estate Management Overview*

HNG-X Estate Management comprises:

The Management, registration, storage, and the supply and installation, of permitted configuration information for Post Office branches and their equipment.

Some items of equipment e.g. the PinPad and items of Branch Configuration data e.g. the office trading hours, are delivered by business application functionality or Reference Data. Current relevant equipment includes the counter and branch router.

4.2.3.3 *Main Components*

The following diagram Figure 20 summarises the main components:

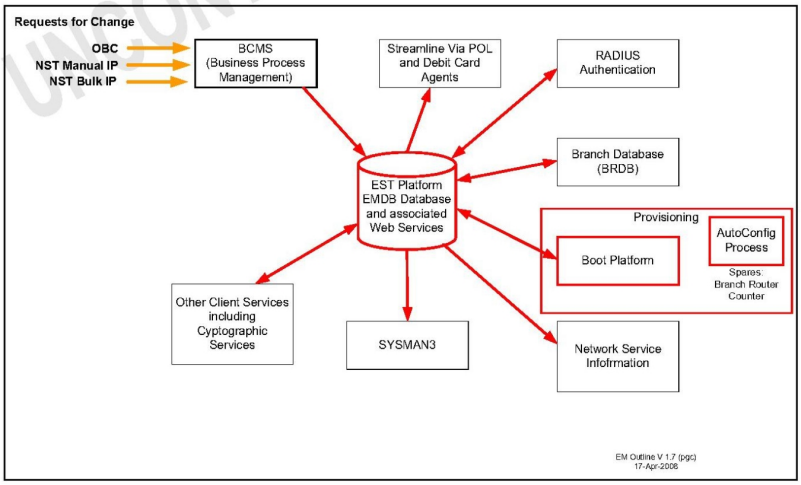


Figure 20

Estate Management Target Architecture

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The red lines identify the scope of Estate Management.

The key points:

- BCMS, the Branch Configuration Management System, is hosted in a resilient workflow server configuration positioned within the Fujitsu Services Corporate Network providing change management facilities into the Production Environment for the OBC team and managing internal and external suppliers, scheduling, customer requests, billing and invoicing. It contains processes, rules and links to external suppliers that fit within the Corporate Business environment rather that a strictly change controlled production environment.

- EST, the Estate Management Database and web Services platform, the repository for permitted branch configuration items comprises 3 elements:
- The EMDB Database, A flexible repository for configuration data stored in a metadata based schema.
- MTAS, the Mid Tid Allocation Service, provides branch and terminal identity information used in Debit Card transactions.
- Web Services Layer, services EMDB Endpoint Clients with configuration information from the EMDB database.
- EMDB endpoint Clients, these comprise systems that require EMDB data to maintain current information on branch estate configuration and include counters in live operation.

- Boot Platform - this provides the means to deliver personalisation data to Gold Build Branch Routers or Counters these contain configurations and applications on the Counter that initiate the installation process.
- Counter Auto-configuration - is the set of components resident in a counter that is invoked when the counter is first installed. It calls into the data centre to a peer Auto-configuration component (on the Boot Platform) and after authentication it is provided with its personalisation data which it applies to the counter subsystems that requires dynamic configuration
- Branch Router Auto-configuration - is the set of components that is invoked when the router is first installed. It calls into the data centre to a peer Auto-configuration component (on the Boot Platform) and after authentication it is provided with its personalisation data which it then applies.

UNCONTROLLED IF PRINTED

4.2.3.4 Estate Management Systems

In the Data Centre (IRE11):

- EMDB Server - Estate Management Database Server – the Registration Authority for the management and storage of the Permitted Branch Estate Configuration data at the Infrastructure level.
- Boot Platform - Part of the Auto-configuration solution for the installation and spares replacement of Branch Routers and Counter PCs.

In the Corporate Domain

- BCMS Server - Branch Change Management Server hosting a Fujitsu BPM instance (BRA01 & LEW02)

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- EMDB Users, BCMS Client Workstations (using a Web front-end) in CRE02 are used to deliver changes to EMDB.

Within Branches the target systems that subject to AutoConfig processes are:

- Branch Router - Uses Branch personality data supplied by Estate Management via the AutoConfig process.
- Counter - Uses Branch personality data supplied by Estate Management via the AutoConfig process.

The diagram below Figure 21 shows a simplified network diagram overlaid with external data flows for ESTATEMAN2:

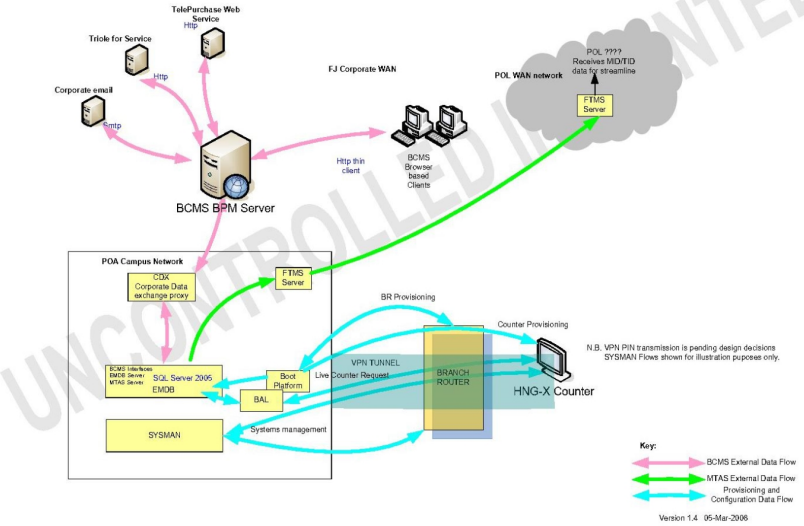


Figure 21

Network Diagram – overlaid with external data flows for ESTATEMAN2

4.2.3.5 *Estate Management Operations*

The functions are:

- Add (open) Branch.
- Add an item of equipment (e.g. counter).
- Remove equipment.
- Close Branch.
- Change an equipment attribute.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.3.6 System Operations

- Day -10 operations are limited to the supply of MTAS Service data to Streamline, via Post Office supplying Merchant and Terminal Identifiers.
- Day -1 operations for the majority of Branch operations; these are supplied into EMDB every evening by BCMS and represent the operational state for the Branch Estate for the following day. This operation is scheduled by BCMS for 19:00 hours every evening.
- Real time operations are instigated by BCMS for contingent purposes such as remedying incorrectly managed change or accommodating late change or system malfunction

4.2.3.7 Estate Management interfaces

The data flows and their associated interfaces are as follows and are documented in DES/SYM/IFS/0003 EST Interface Specification.

EMDB has a view of Reference Data from the Branch Database, it also has legacy views from RDMC (MTAS)

- EMDB supplies interfaces for clients to invoke services:
- Boot Platform (Counters)
- Boot Platform (Routers)
- Boot Platform (Radius)
- SYSMAN3 (Routers)
- SYSMAN2+ (Counters)
- Radius Servers
- BCMS Use Cases
- Estate Management delivers material or triggers actions
- MTAS data deliveries MID/TID mappings to the Debit Card Agents via shares scheduled by TWS.
- MTAS data deliveries to Streamline via POL.
- SYSMAN3 TPM - Router Registration – Inventory reported via Windows Events from Boot Platform.
- Branch Database – EMDB delivers current operational view & Reconciles reference data derived information.

4.2.3.8 Estate Management Server (EST)

The Estate Management Database (EMDB) is based on a single SQL Server in IRE11, and is a combined database and set of tools (stored procedures, triggers). The EMDB is the registration authority for the permitted Branch Estate values, other values used in production of configuration data for endpoint components are taken from other sources, primarily Reference Data.

Change data is injected into the EST by BCMS, this triggers the EST to generate all updates to relevant data.

4.2.3.9 EST Endpoints

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The EST Endpoints are predominantly provided by java clients that retrieve endpoint information from the EST via SOAP calls.

The following table indicates in summary the Endpoints:

Endpoint	Topic Architecture	Data
Branch Database	Branch Database	Branch codes and IP addresses. Advance notification of opening/installation dates.
NNM	Network	IP Address data
DNS	Network	IP Address & name data
RADIUS	Network	Branch codes, IPS, BR Serial number and CHAP data.
Boot Platform	Estate Management	RCFs, BSFs
Live Counters	Counter	Numbers of counters, NST data, provisioned via BAL
RDDS	Reference Data	Numbers of Counters.
SYSMAN3	Systems Management	RCFs

Estate management Endpoints

UNCONTROLLED IF PRINTED

4.2.3.10 EST Endpoint Clients

These are the target systems for the configuration material; there are three types of Estate Management endpoint client Equipment.

- Branch Equipment Routers, counters and future branch equipment are provisioned by the Router BootServer Service on the Boot Platform. Note that once the Router BootServer Service registers the details of the Branch Router with SYSMAN3, the router is subsequently managed by SYSMAN3 (TPM).
- Network Equipment Network infrastructure such as DNS, NNM and the LNS routers need to know about counter and branch router ip addresses for monitoring, diagnostic and directory purposes.
- Data Centre Equipment - RDDS has a requirement to be aware of the status of opening and migrating branches and must therefore know in advance (day -1) of their intended opening;

4.2.3.11 Boot Platform

The Boot platform exists to support the provisioning of new Branch Router equipment into Branches. It hosts the following functions:

- The Radiator RADIUS Service which consists of a suite of customised PERL Scripts that support the Branch Router AutoConfig processes. Router Boot processes are triggered following successful authentication of a connection request to the boot radius by a Gold Build Router.
- Branch Router Boot Server Service.
- This is triggered by the Radiator RADIUS Service and configures the Branch Router.

Boot Platform functionality is described in DES/SYM/HLD/0037 “Autoconfig HLD”

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.3.12 Boot DMZ

The Boot Platforms reside in a single Boot Domain DMZ (De-Militarised Zone) with dedicated access points to support the installation of the Branch Router. Gold Build Branch Routers are configured to connect into the boot DMZ over PSTN as the primary connection method for configuration purposes; this network service supports the identification of the Service Termination Point Using CLI.

ADSL is the predominant primary communications method, used for normal business, utilising this method CLI is also be available for most ISDN equipped sites. Using known service termination points permits the identification of the Branch at which the unit is to be deployed.

For installation of counters, the Branch Router is connected into the main Data Centre access LANs already.

4.2.3.13 MTAS Access

EST hosts the MID/TID Allocation Service (MTAS) with data. This is made available in advance of the target change date by BCMS and RDDS. With the introduction of HNG-X, the generation of MTAS material for Counter Training Offices (CTOs) is suppressed; RDDS also excludes CTOs from its MTAS view and this ensures that no MID/TID details are ever assigned.

4.2.3.14 Scheduler Functions for Estate Management

TWS is used to:

- Schedule backups of the EMDB database.
- Schedule Backups of the MTAS database.
- Schedule MTAS and other applications that need to be invoked on a periodic basis.
- Schedule the activities of any clients that have a dependency upon the TWS Schedules.

UNCONTROLLED IF PRINTED

4.2.4 Reconciliation Services

4.2.4.1 Management Information Services (MIS) Overview

The Management Information Service consists of three primary databases, i.e. the Data Reconciliation Service, the Transaction Enquiry Service and the Data Warehouse, all of which reside on the Database Server (Main Host).

The POA Management Information Service does not have access to the APOP Voucher database which resides on the Database server. (An APOP Administration Service is available within Post Office Limited at their Northern Data Centre)

4.2.4.1.1 MIS Clients

FUJ00232658

~~There are three MIS clients available in Bracknell, and for contingency purposes one MIS clients are available at STE04, for reconciliation purposes~~The MIS Client Application facilitates access to the Data Reconvciliation Database and is accessed via Remote Desktop connection to the Secure Access Server.

The TESQA is used by POA Service Delivery to access a read-only view of Network Banking Transaction details.

TESQA is not available via a MIS client (due to a design omission relating to intranet access via red LAN that doesn't exist).

4.2.4.2 The Data Reconciliation Service (DRS)

The DRS provides the end to end reconciliation for NWB and DCS (Electronic Fund Terminal PoS) transactions performed at the Post Office counter. The transactions are held in the Branch Database and transferred as C12 XML messages to the DRS system. The transaction data is also transferred to TPS from the Branch Database and from there it is sent to the DRS as C112 validated data. The DRS generates DCS C2 messages from the C12 for transfer to ~~Streamline~~ Globalpay which in turn cause confirmation messages to be sent back to the DRS. Reports are produced for Post Office Limited and this is illustrated in the diagram in the next section. The data for NWB transactions is also made available to the Transaction Enquiry Service.

The DRS Workstation application is used to query the data held in the DRS tables ~~and remains unchanged~~.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The shaded area in the diagram Figure 22 below shows the scope of DRS.

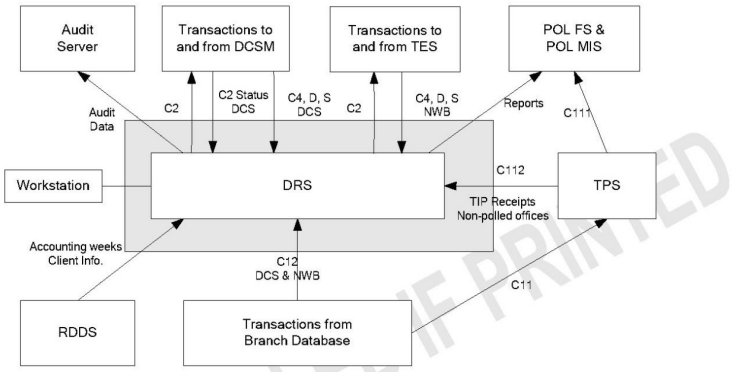


Figure 22

Scope of Data Reconciliation Service

UNCONTROLLED IF PRINTED

4.2.4.2.1 Reconciliation Reporting – HNG-X Outlets to DRS

There are two types of message flow between HNG-X Outlets and the DRS.

- ~~Individual~~ Confirmation [C12] transactions. These are transferred ~~throughout the day by the NBX Confirmation Harvester Agent. Harvesting is done on a continuous basis, with the [C12]s loaded into the DRS in recoverable commitment units, following normal replication of the [C1] messages within the EPOSS transactions~~to the Data Reconciliation Service at the end of each Trading Day
- EoD transaction processing of [C11] transactions. These are transferred to the TPS Service at the end of each Trading Day

  ~~As part of the normal EoD Campus processing, TPS transaction harvesting occurs following receipt of the EoD marker from Outlets. This provides a delineated set of completed transactions up to the Outlet declared EoD, which forms the basis for transaction reporting to TIP. (Subsequently such transactions also provide the basis for calculating the Cash Account report for TIP.)~~

- NBX and DCS transactions included within the TPS harvesting ~~is~~are forwarded to the DRS to provide an aggregated Outlet position to support reconciliation. Such transactions are consistent with the Outlet reported transactions sent to ~~TIP (other reconciliation measures detect inconsistencies within the TIP reporting stream), and include the intended Cash Account Period (CAP) in which they are accounted for by PO Ltd (as part of the TIP processing). See DES/APP/HLD/0033 for more information~~Credence and POLSAP.

Commented [AP2]: SOS to comment as to whether or not Reconciliation files travel through TIP remote or in fact EDG/ SAP?

4.2.4.2.2 Reconciliation Reporting – POA DRS to PO Ltd

A number of reports are generated, some daily and some weekly, as defined in HNG-X version SVM/SDM/SD/0020 – Network Banking End to End Reconciliation Reporting.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.4.3 Data Warehouse

- Figure 23 below depicts the Data Warehouse inputs. The individual Host Database systems produce SLT or PM data extracts as flat CSV files[1]. The Data Warehouse loads and consolidates this data as part of its' overnight process. A generic reporting mechanism detailed in (ref. DES/APP/HLD/0049) will be installed in the host database systems and configured to make suitable data extracts to be imported into the warehouse. In many cases there is already a mechanism which extracts similar data for SLT and PM measurement. SSC is responsible for to ensure that the files reach the REC team by supporting the file transfer route via the DXC. REC team produce the reports.

  See DES/APP/HLD/0082 for more details.

  The Databases that reside on the Solaris Main Host (Database server) are:

  TES, APS, TPS, LFS, Web Service, BRDB & RDMS (RDMC and RDDS databases) services.

UNCONTROLLED IF PRINTED

[1] Note: Performance and Service Level Measure reports are migrating to HORIce as part of CP1305.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

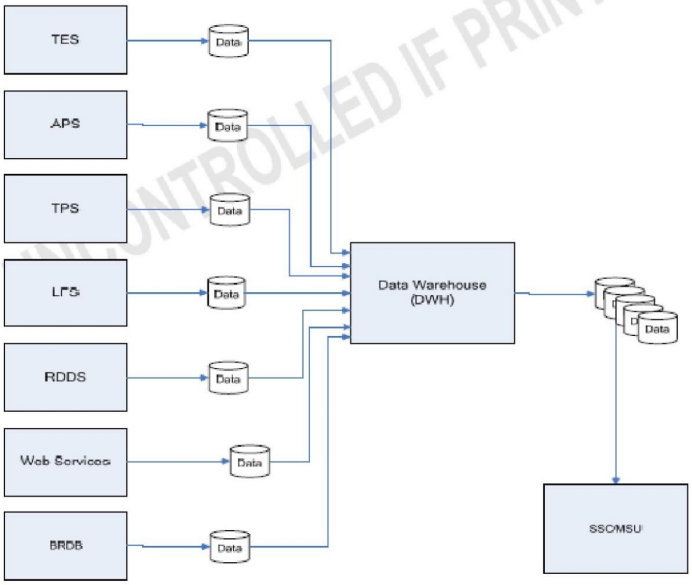


Figure 23

Data Warehouse inputs

The overall structure and functionality for contingency purposes may be represented as follows.

The "data warehouse process" is the set of operations/processes required to source, load, manage and publish data in the data warehouse. Figure 24 gives a conceptual overview of the processing required to operate the POA data warehouse.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Data Warehouse Conceptual Process Architecture

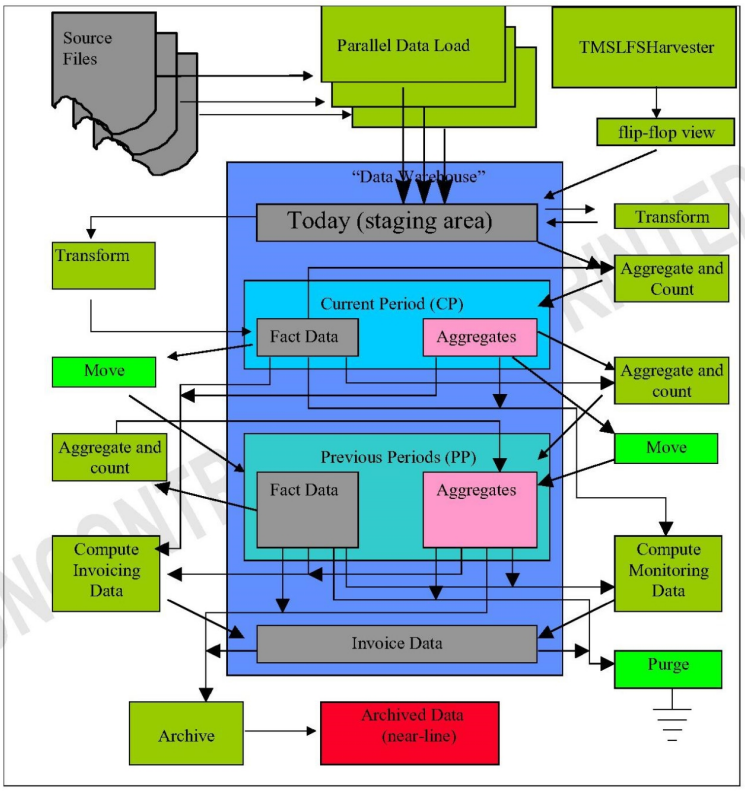


Figure 24

Data is provided by the source systems in the form of flat files uploaded to a dedicated area on the data warehouse. The source files are then loaded (in parallel, where appropriate) into a staging area within the data warehouse. This staging area holds a complete day's worth of data. Any transformations which may be required (e.g. derivation of values etc) is performed on loaded data, and not as part of the load processes. The staging area is normally the data source for processes which pre-compute daily aggregated totals. These pre-computed totals are required by invoicing (invoice data) and to satisfy end-user queries. The data in "today" is transformed into a dimensional structure and moved into Current Period (CP). CP stores the data pertinent to the current period while it is being built up over the course of the week. Once the CP has been completed, the data is moved over to PP (this move requires no transformation). After the data has been moved, it is archived. Archived data is used by the "near-line" mechanism to allow data which is no longer on-line to be queried. CP and PP are the data sources for processes which pre-compute aggregates of grains greater than a single day (i.e. weekly and monthly)

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The DFD feed is provided from an interactive harvested agent.

4.2.5 End to End Reconciliation Service

The following outputs from the Data Reconciliation Service (DRS) constitute the End to End reconciliation service:

1. Banking and Related Services transactions, which includes DCS and ETS
2. Automated Payment System (APS)
3. Transaction Processing System (TPS)

The end to end transaction flows are supported by validation processes which verify that the transactions processed by the APS Host are consistent with the transactions included in each Client Transmission File and with the CTS sub-file sent to Post Office Ltd.

This validation is carried out for the volume of normal transactions and the value of all transactions only in each of these files. Any differences in this reconciliation will cause an operational alert to be raised and the appropriate file delivery to be suspended.

A Validation Status report will be produced as part of this validation process and the results of this notified to Post Office Ltd.

Reconciliation reporting operates on a seven day a week basis regardless of the Client file transmission schedule (which may, for example, exclude weekends and bank holidays). These Rec files are delivered via the DXC to SSC server poasmpdev which is then accessed by the Reconciliation team. In principle, reconciliation reporting totals volume and value for transactions. It includes reversals by adding volume and subtracting value.

UNCONTROLLED IF PRINTED

4.2.6 POLSAP Development and Test/QA Services

The output reconciliation files (.ble) are delivered to SAP XI and transformed into idocs which in turn updates POL SAP.

The Post Office Limited Financial Services SAP service consists of three elements:

a Production service, a Development service and a QATest service.

The POLSAP Production service is documented within the HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002).

The POLSAP Development and QATest service have been classified as supporting services and are therefore included in this plan.

The POLSAP Development Service and the QATest Service is hosted on a platform in the Fujitsu IRE19 Data-centre.

In the even of a disaster at IRE11 or a major incident occurring with the Production server, the Development/QATest server at IRE19 may be brought into use to provide a disaster recovery environment. Refer to HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002).

The POLSAP Development and QATest services are normally available Monday to Friday from 08:00 to 18:00. However either could be available at other times by agreement.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

There are no business continuity or disaster recovery requirements for either the POLSAP Development or Test/QA services.

Post Office Limited users can run and print POLSAP financial reports from the POLSAP Production system located in IRE11, by access through the POL Northern Data Centre. Additionally, Post Office Limited users are able to develop and test changes on the POLSAP systems in IRE19, again accessing these systems via the POL Northern Data Centre.

In the event that the POL Northern Data Centre is unavailable, Post Office Limited may decide to invoke POL NDC disaster recovery for the TIP remote Gateway at SunGard Hounslow and for EDG gateway at Prism's DR data-centre at Maidstone. POL and Prism users can then access the services in IRE11 and IRE19 via Hounslow.

Duty Manager Notes:

1. In the event of a POA OOH Duty Manager being informed of ' P1' priority incident on either the POLSAP Development and Test/QA services they are to inform the POA Client Interface Service Delivery Manager.
2. Post Office Limited has accepted a POLSAP 'disaster recovery' fail-over time of 48 hours and the unavailability of the POLSAP QA-Test service.
3. It is Post Office Limited decision whether or not to invoke the fail-over to their SunGard DR site at Hounslow and the time for full invocation is 48 hours.
4. In the event Post Office Limited invoke SunGard the SAP-Basis support team need to reconfigure IP addresses for POL print server at Hounslow.

UNCONTROLLED IF PRINTED

4.2.6.1 *POLSAP Hosting Development Service*

The Development server at IRE19 is a Fujitsu-Siemens PrimePower 450, running Solaris with ESF. Veritas Volume Manager is used to mirror the boot device and to provide redundant multi-pathing over dual fibre channel connections to the SAN and thence to the EMC disk array.

The development server supports one SAP instance. A PRISM development instance called PLD. This forms part of the release process for fixes from PRISM (Xansa).

All application backups are performed by presenting EMC BCVs to the backup server. Each instance presents the database and file systems (e.g. archive redo logs) separately.

4.2.6.2 *POLSAP Hosting XI QAtest Load Service*

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The SAP Hosting XI Load service in IRE19 comprises a SAP NetWeaver Central Instance and 1 SAP NetWeaver Application Servers

The NetWeaver servers are Fujitsu-Siemens PrimePower 450, running Solaris 9 with ESF. Each server has 4 CPU (1.1GHZ SparcV64) and 8 GB RAM. Veritas Volume Manager is used to mirror the boot disk and to provide redundant multi-pathing over dual fibre channel connections to the SAN and thence to the EMC disk array.

The Central Instance has Disk storage allocated on the EMC, and is backed up by presenting EMC BCVs to the backup server. The backup server presents the database and file systems separately.

The QATest XI server also provides DR capability; it has a spare set of boot disks which are restored nightly from a backup of the production XI server which enables this server to be invoked as the production XI Central Instance in the event of a Business Continuity incident.

The QAtest NetWeaver application server is connected to the NetWeaver Central Instance in the event that a Business Continuity event is declared, the server has the capability to connect to either Production or QATest Central Instance but under normal conditions the QATest connection is active.

4.2.6.3 POLSAP Hosting QATest Archive Service

The QATest Archive service runs on a Fujitsu-Siemens PrimePower 450, running Solaris with ESF. Veritas Volume Manager is used to mirror the boot device and to provide redundant multi-pathing over dual fibre channel connections to the SAN and thence to the EMC disk array. The archive service uses a software package from Opentext (IXOS for SAP).

The QAtest Archive service is located in IRE19 and the archive data is held on EMC Centera system. The IXOS application maintains an Oracle database on the archive server which maps SAP archive object ids to the Centera. The QATest archive server maintains a different data partition on the Centera from that used for production archive data.

All application backups are performed by presenting EMC BCVs to the backup server. Each instance presents the database and file systems (e.g. archive redo logs) separately.

UNCONTROLLED IF PRINTED

4.2.7 Network Services

4.2.7.1 Branch Network Service

4.2.7.2 Branch Network Service

- The Branch Network Service is responsible, using appropriately trained operational staff, for performing the day to day operational control and management of the following components of the Branch Telecom Infrastructure:
  - The Wide Area Network (WAN) for connected Branches, i.e. the connection between the Branch Infrastructure and the HNG-X Central Infrastructure. This excludes BFPO where the connection is provided by the local British Forces.; and
  - The connection between the router and the telecommunications socket in the Branch.
  - The connection between the POMS and the router in the branch.

- The Branch Network Service is based on remote unattended principles, i.e. monitoring tht seeks to minimise interruptions to the normal business operation of the Branch Inrastructure.
- Communications Incidents can be identified by either the Branch or Fujitsu Services following monitoring of the Branch Telecom Infrastructure.
- All Branches will be equipped with a backup network based upon mobile communications via the 2G/3G router. The use of this backup resilient network will be dependent upon a 2G/3G signal being available.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- The Branch Network Service is responsible for the measurement and reporting of Branch and Counter Availability Service Level Targets (SLTs), which will include the effect of Branch Telecom Infrastructure Incidents and Branch Hardware failures across all items within the Branch Infrastructure and failures within the HNG-X Central Infrastructure.
- The Branch Network Service is also responsible for the measurement and reporting of the Reliability SLT and the call to fix SLT in respect of Branch Telecom Infrastructure faults.
- The Branch Network Service is a service internal to Fujitsu Services and is available 24 hours per day, every day of the year.

- Post Office may contact the Branch Network Service team during the hours of 09:00 to 17:30 Monday to Friday, excluding Bank Holidays.

4.2.7.2.1 Time to Repair

- Incidents relating to the Branch Telecom Infrastructure which prevent an individual Branch from using the HNG-X Application shall be resolved in accordance with the following SLT.
- The location of each Branch is classified as either local or remote. All Branch changes may be subject to Operational Business Change. A new Branch location will assume the same SLT and LDT as the one it replaces unless it's local or Remote status is changed, in which case the SLT and LDT to be applied will be agreed by Fujitsu Services and the Post Office.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- The call to fix SLT for the Branch Network Service following receipt of a call to the Service Desk relating to the Branch Telecom Infrastructure is identified in the table below:

Branch Location	SLT (Hours of Downtime)	
Local / Remote Priority A	95% resolved in less than 4 hours	100% resolved in less than 6 hours

4.2.7.2.2 Maintaining Contact with the HNG-X Central Infrastructure

Branches use a resilient network where there is a 2G/3G signal available, should the primary communications network be unavailable. There are no further Business Continuity arrangements to ensure Branch Telecom Infrastructure connectivity.

4.2.7.3 Branch Service Structure

Approximately 11,212 Post Offices (as at July 2014) are linked to two Fujitsu Services (Post Office Account) Data-centres by one of the network service types defined in the Table below, which also defines the contingency routing and/or fail-over network services types which are available for each service type.

UNCONTROLLED IF PRINTED

NST	EX_NST	Fallback EX_NST	Comms Type and description

FUJ00232658

22	22		VSAT
	25		BFPO with ConnectVPN
24	24		Bronze ISDN (DoD)
	23		ConnectVPN
	26	23	POMS with ConnectVPN
29	29		Silver ISDN (nailed up)
	23		ConnectVPN
	26	23	POMS with ConnectVPN
33	33		ADSL
	35		Mobile PO (VANN)
	26	23	POMS with ConnectVPN but branch is defined as NST-33 as no longer on ISDN
	36	33	POMS with ADSL
34	34		ADSL with ISDN backup
	26	23	POMS with ConnectVPN but branch is defined as NST-33 as no longer on ISDN
	36	34	POMS with ADSL

Branch Network Service Types

UNCONTROLLED IF PRINTED

4.2.7.4 Client Links

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The Client links are defined as those circuits conveying data between the Fujitsu Services POA Data-centres and:

- the Post Office Limited data-centre in POL NDC, e.g. for LFS, APS, POLSAP and Reference Data;
- all AP Client data centres, including EDS for the Card Account Receipt Service.

4.2.7.5 *The Branch Resilient Network (BRN)*

The Branch Resilience Network provides the following coverage:

- An automatic ISDN backup network for the largest ADSL branches
- A backup on demand GSM service that covers all the ADSL and ISDN sites This would involve an Engineer turning up within 48 hours after a network outage had started and installing the backup network. Once the fault had been fixed, the backup network GSM Modem would be removed.
- The ability to use the backup network, via GSM, for branch relocations if the main network had not yet been installed in the new location
- The backup network would use the same IP address as the main network. This means that all Post Master functions will work, albeit with less bandwidth than normal.

For full details please refer SVM/SDM/SD/0011- Branch Network Service Description

4.2.7.6 *Branch Router Overview*

The Branch Router selected is the Sarian DR6410 model and has an external (to the router) glass mount antenna which is connected via a cable from the router to a suitable position within the post Office counter secure environment. It has LAN switch functions, a selection of WAN interfaces, LAN & WAN routing functions including ADSL, ISDN and Wireless WAN (2G/3G) interfaces, built in. PSTN connectivity is used via an external modem connected to the serial port or USB port where required.

The Branch Router has four Ethernet ports performing the LAN switch function, two of which are used for branch LAN connectivity. The other two are reserved for future use.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

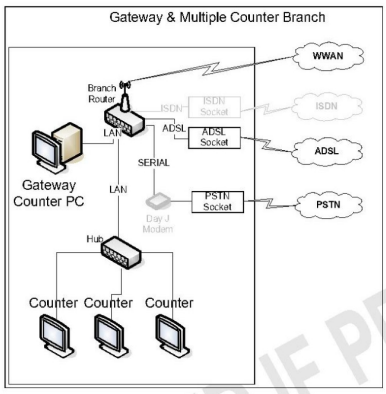


Figure 25

Physical Overview of Gateway with Multiple Counters & Branch Router

UNCONTROLLED IF PRINTED

4.2.7.7 Branch Network Overview

The ADSL network is the primary connection type. A new Wireless WAN data technology has been introduced using a 2G & 3G services from Orange and Vodafone. WWAN provides a backup connection type for the entire branch estate (where coverage permits). ISDN is retained in required sites as the backup connection type. ISDN connectivity is being phased-out in favour of ADSL or WWAN connection types. Exceptions to this standard approach to connection types are where the primary connection type is unavailable, such as Hull and very remote areas where ISDN or VSAT are preferred (ISDN is preferred over VSAT if available).

It is envisaged that the majority of branches have two connection types (ADSL for primary and WWAN for backup).

The VPN servers in the data centre (running NT under MSVS are configured to accept VPN traffic from the Gateway PCs WAN IP address. With the Branch Router in place the Gateway PC is required to handle the VPN connection, but will connect via its LAN interface to the router.

This diagram shows the logical connectivity from the Branch LAN to Data Centre

© Copyright Fujitsu Services Limited 2014

FUJ00232658

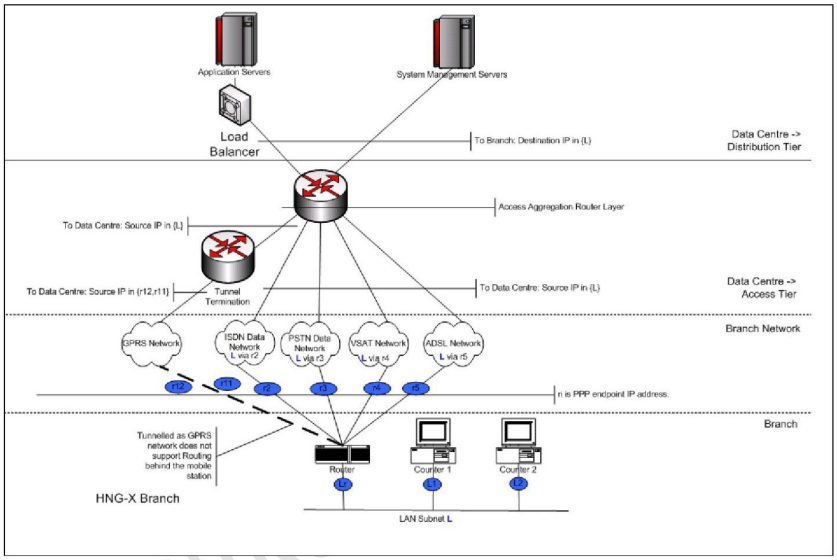


Figure 26

Logical connectivity overview Branch LAN to Data centre

AEI Interim Branch Connectivity

Design: DES/APP/DPR/0671

TIS: DES/NET/TIS/0731

Detailed Network Design AEI Interim Connectivity Solution: DEV/INF/LLD/0982

AEI Integration TIS: REQ/INF/TIS/0001

POMS HLD : DES/SYM/HLD/1886

Post Office is providing the Application Enrolment and Identity (AEI) service to some of its branches. One or two AEI terminals per branch capture the data and send it to Cogent data centres at Farnborough and Bristol.

Fujitsu provide, manage and monitor the transit network between the Post Office branch and Cogent data centres.After the implementation of POMS solution Fujitsu would support the POMS device along with the existing ones.

The Farnborough data centre is the primary data centre with the Bristol data centre operating as a failover (DR) site. Resilience is provided between data centres via a common layer 2 LAN for the benefit of branch connectivity only. In the event of Cogent invoked DR, branch AEI connectivity will automatically failover to the Bristol site.

The following diagram outlines the basic architecture of the POMS solution which is the subject of the Design Proposal (DES/SYM/HLD/1886). It depicts the AEI Counters connected to the Post Office Managed Switch and using the Branch Router to reach the AEI Data Centres.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

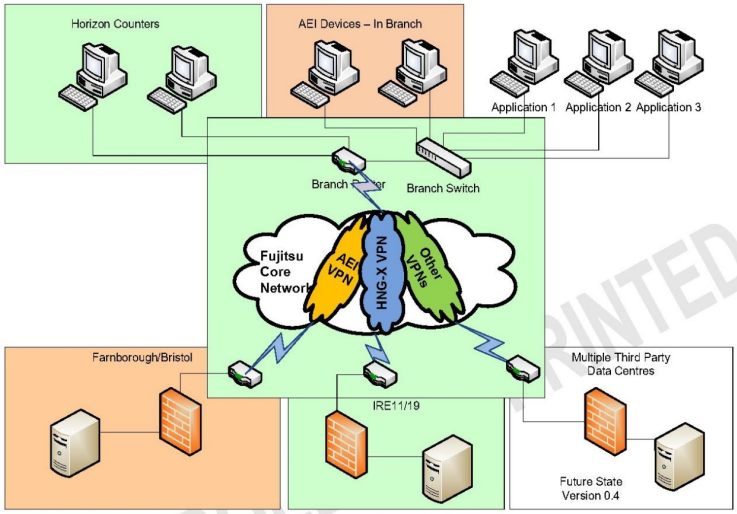


Diagram Source : DES/SYM/HLD/1886

UNCONTROLLED WHEN PRINTED

4.2.7.8 Wireless WAN Service

The Wireless WAN service is used as the primary connectivity for mobile branches, where no fixed line communication service is possible, and as a backup network type in the event of the primary network at a fixed branch, namely ADSL, ISDN or VSAT connection failing.

The Orange managed service utilises two private Ethernet based leased circuits into two data centres, namely SDC01 (30Mbps MegaStream Ethernet) and TCY02 (100Mbps LES). Orange provide managed MPLS CE routers (Cisco 2811) which terminate the Ethernet services between the Orange MPLS PE and CE routers. The Ethernet circuit from Orange into the TCY02 data centre is the preferred for LIVE traffic as this has the greater bandwidth. This also coincides with the primary route to the POA data centres, via the VODAFONE MPLS WAN, being in TCY02.

In addition to the Orange service there is another service from Vodafone which utilises an IPSEC tunnel from the Vodafone MPLS network, over the internet to a Cisco 2811 router in TCY02. This test IPSEC solution will be used to provide the concepts and connectivity for a Vodafone final service that is analogous to the Orange managed service. All Vodafone test traffic will be presented over this test IPSEC solution until the service is validated and a fine Vodafone managed service utilising dedicated leased lines for the live environment and a single dedicated leased line for test.

4.2.7.9 Data Centre LANs

© Copyright Fujitsu Services Limited 2014

FUJ00232658

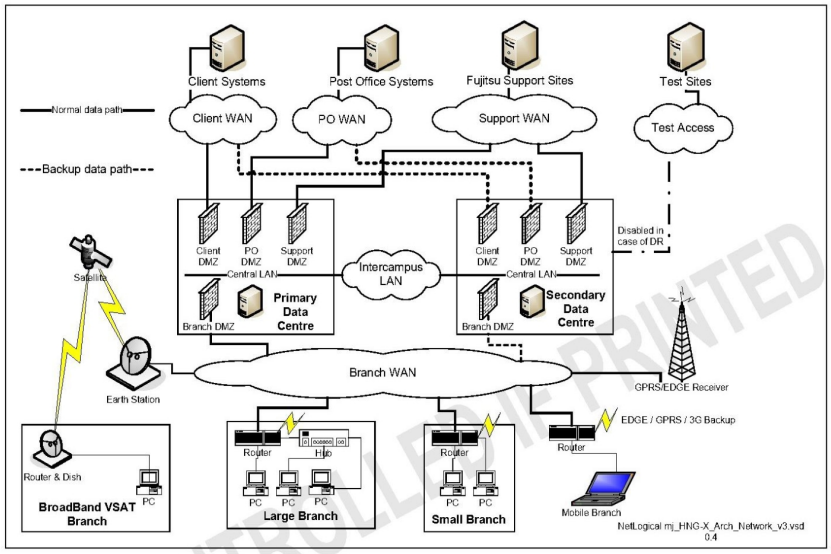


Figure 27

Overall view of the HNG-X Target Network solution

The solution comprises the following network components:

- Data centre LANs (Production and Test)
- Core LANs
- DMZs
- Branch
- Client (Santander, CAPO, Vocalink, DVLA, HMS(HSBC Merchant Service), EPay)
- Post Office (Huthwaite, Sungard)
- Support (CRE02, WAR13, BRA01, LEW02, STE04, IRE11, IRE19)
- Inter-data centre WAN connectivity

4.2.7.10 WAN Connectivity - Fujitsu sites to IRE11 & IRE19 Data Centre

WAN connectivity between the POA data centres and Fujitsu core sites is provided using VODAFONE IP Connect VPNs. These comprise multiple L3VPNs (RFC2547bis). The live traffic for both HNG-X and Horizon traffic shares a common VODAFONE VPN. Test traffic however, will have a dedicated VODAFONE VPN.

VODAFONE provide and manage the CE router at each site and present individual VPNs as VRFs on each CE. Routing between the PE and CE routers using eBGP is managed by VODAFONE. BGP will also be used for routing between the VODAFONE CE routers and the Cisco 7304 VPN Crypt routers. As the Utimaco VPN servers are considered network devices and therefore operate in an active/active manner,

© Copyright Fujitsu Services Limited 2014

FUJ00232658

there is no requirement to steer traffic towards a particular data centre (IRE11/19). Triangulation of access to IRE11 and IRE19 is provided using intercampus VLANs and provides for failover between sites.

Live branch traffic will be steered to ingress/egress SDC01/TCY02 via the TCY02 CE router, with test counter traffic steered via the SDC01 CE router. The access circuits for both sites are dimensioned to carry both live and test traffic during failover.

4.2.8 Fujitsu Shared Services

Fujitsu Services now provides many business solutions using a shared service model. This enables Fujitsu to provide a more cost efficient service to all customers by sharing common facilities and functionality.

4.2.8.1 Shared Data-centres

The two Irish data centres, IRE11 and IRE19, which are used to provide the POA HNG-X solution, are shared facilities. Non-POA equipment is kept at both locations in order to provide services for other Fujitsu customers. In addition the POA solution also makes use of other Fujitsu Shared data centres in other parts of the UK as part of the total solution, including TRIOLE for SERVICE (TfS) and ConnectDSL.

4.2.8.2 TRIOLE for SERVICE (TfS) – Shared Incident Management System

TfS is the Fujitsu Shared Services Incident Management system being used by POA and other Fujitsu customers.

The TfS primary system is located at SDC01 (Fujitsu Southern Data Centre) and is accessed via the Fujitsu Corporate network.

Engineering incidents, which are to be passed into FMS for resolution, are transferred from TfS over the OTI link into the D1 system and then to CRISP /Touch system.

There are two application servers operating as a single system. The loss of one server will cause a loss of capacity and resilience. All users will be able to run from a single server but those users that had been logged into the failed server will need to log in again to be connected to the remaining server. There is a backup system in SDC02, for use following the loss of the primary system which is kept up to date via data log file shipping.

4.2.8.3 ConnectDSL – Shared Service - SDC / TCY

The ConnectDSL Shared Service provides the connections to Post Office Branches from the Fujitsu Data centres in the south of England (Southern Data Centres). This service is also used by other Fujitsu customers via common equipment and applications.

Each branch access method terminates on dedicated LNS platforms within the SDC01 and TCY02 core sites (VSAT does not use L2TP and therefore the platform is not strictly a LNS, but the general principle remains). Bootloader access is an exception to this where shared LNSs within the VODAFONE network are used.

Branch sessions are Radius authenticated. The termination platforms all reside on a common LAN infrastructure between SDC01 and TCY02 (referred to as the 'shared LAN'). Live traffic is segregated from test traffic using VLANs. The VODAFONE CE routers also currently reside on these VLANs. The CE routers present VPNs as VRFs that in turn are associated with the VLANs.

Two layers of Radius are employed. A 'platform Radius' is used by Fujitsu Core Services within SDC01/TCY02 to identify the traffic type (live branch or test counter) and thereby which VLAN to forward on. Further Radius platforms, under POA control, within IRE11/19 are used for authentication and accounting.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The impact of loss of datacenter have written in SVMSDMPLA0002- HNGX services business continuity plan, in section 11.2 , Item number 201 to 221.

4.2.8.4 *Fujitsu Global Cloud Platform(Salesforce)*

Post Office are at an early stage of utilising CRM and the future requirements and scope of integration with the other business systems is unclear. However, significant business benefit had already been identified during trial for Financial Specialists and Post Office were keen to replicate this benefit across all the FS users. To allow Post Office to progress CRM whilst able to scale or even change future requirements was key to Fujitsu's proposed solution. The Fujitsu Global Cloud Platform was selected as it provides no long term commitment to the deployed infrastructure, can be quickly scale up or down. Also given that salesforce.com is an internet based cloud application, the use of the FGCP was appropriate for this solution.

Production services are provided from the STE10 data centre in the UK. Customer's access the reserve proxy using a URL (https://salesforce.postoffice.co.uk) and certificate provided by Post Office.

DR services are provided from the FGCP platform in Germany. Customer's access the DR reserve proxy using a URL (https://sfdr.postoffice.co.uk) and certificate provided by Post Office.

The SQL databases used in this solution are replicated onto another SQL server in the DR infrastructure using SQL log shipping facilities. A Remote Routing and Access Server (Windows 2008SE) is deployed to provide routing into the two secure zones and to manage an IPSEC tunnel between the environments.

The impact of loss of datacenter have written in SVMSDMPLA0002- HNGX services business continuity plan, in section 11.2 , Item number 238 to 240.

4.2.8.5 *Cloud Connect VPN service and Cloud connect network service.*

The Cloud Connect VPN service and Cloud connect network service has been design to describe infrastructure which exists outside of the FJ datacenters which host the existing HNGX services in Ireland. For the avoidance of confusion, this infrastructure has no connectivity with HNGX in any way whatsoever.

Provide a transit path for ATOS SISD traffic originating from the public internet secured within an IPSEC VPN. Document Reference is DES/NET/HLD/2476.

Network Sub-System Description:

Atos will connect to TFS using IPSEC VPN over the public internet. The IPSEC tunnel will be delivered using the Fujitsu Cloud Connect IPSEC VPN service and terminate on a RIPE address presented by the shared VPN devices in the Fujitsu TCY01 and TCY02 data centers.

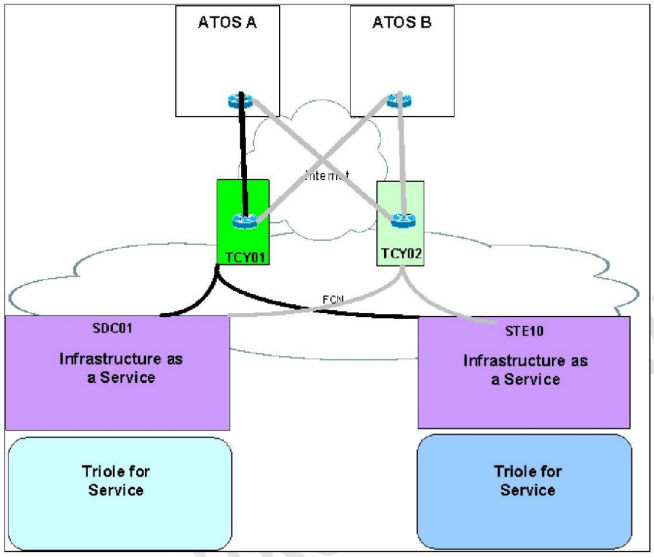
Data from within the IPSEC endpoints will then traverse a new customer MPLS VPN across the FCN to the data centers out of which the TFS service is hosted, namely SDC01 and STE10.

TFS is a mixed component solution in that it consists of an Infrastructure as a Service managed firewall which becomes the transit point for all ATOS and FJ related traffic as it leaves the FCN towards the TFS systems. The TFS systems are themselves contained within a specific TFS customer virtual pod and will be referred to as TFS-PROD and TFS-UAT

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658



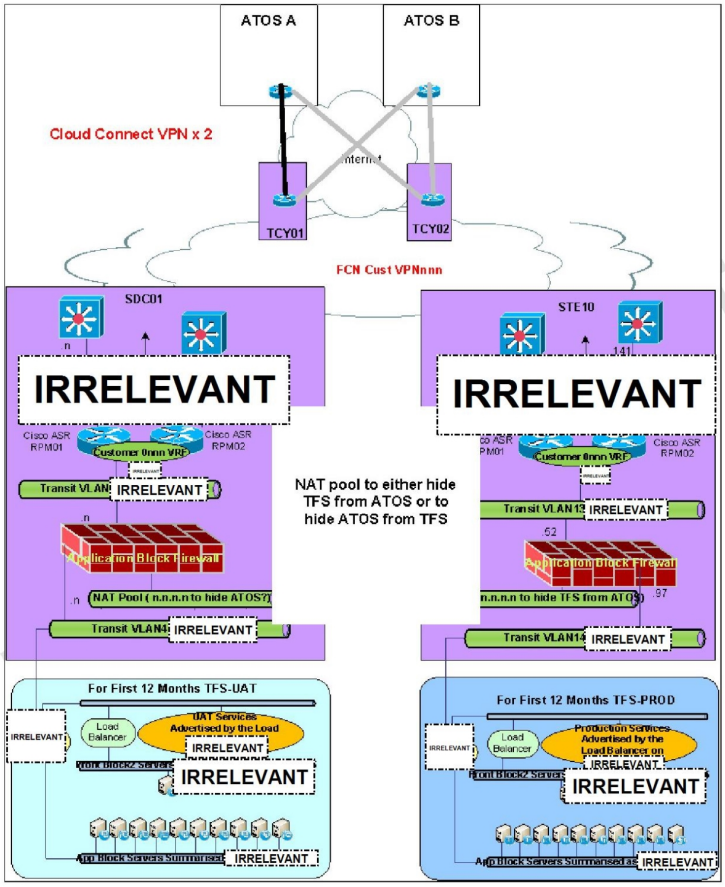
The primary path will be from ATOS A to TCY01 to both SDC01 and STE10 in support of the annual switch of Production and UAT between SDC01 and STE10. Grey links are backup links to be used in the event of the loss of primary path.

Networks:

The network solution is shown below with the *access services* described in red and the purple and blue boxes showing the *IAAS* and *TFS* components of the solution.

© Copyright Fujitsu Services Limited 2014

FUJ00232658



Availability:

In summary:

- There will be two instances of the TfS application – Production and UAT, which are known throughout this document as TfS-Prod and TfS-UAT respectively. These instances are actually images of the virtual servers which are used to host the particular TfS application. The images are stored on (and replicated between) the SANs located at STE10 and SDC01. The details surrounding image replication between SANs and data centres is beyond the scope of this network design document.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- Under normal operating conditions the production image of TfS (TfS-Prod) will be loaded on the IaaS infrastructure at one data centre (SDC01 or STE10) and the UAT image of TfS (TfS-UAT) will loaded on the IaaS servers in the other data centre (STE10 or SDC01).
- There will be a scheduled 'rolling fail over' (approximately every twelve months) whereby the Production and UAT images exchange locations, demonstrating the full DR capability.
- In an actual DR situation where the site running the production service suffers a catastrophic failure requiring fail over, production will fail over to the alternative site; UAT will run concurrently with production at that site, at reduced capacity. This supports a scenario where a site is lost and there will be an extended period of time required to replace it. During this period, UAT may still be required in a limited form

  Note that:

- Disaster recovery (and indeed the scheduled rolling failover) is not automatic - it will be a controlled process with downtime. From a network perspective changes will be required to the ATOS VRFs (at each data centre) which is used to advertise TfS-Prod and TfS-UAT to the customer using BGP.
- Disaster recovery (and the scheduled rolling failover) is not automatic - it will be a controlled process with downtime.

From a network perspective every time it is necessary to fail over TFS -Prod and/or TfS-UAT between data centres it will be necessary to make the routing changes

UNCONTROLLED IF PRINTED

4.2.9 External Suppliers

4.2.9.1 VODAFONE Network

The core VODAFONE network has been designed to provide resilience through the deployment of SDH technology. The network is made up of a series of interlocking rings, should one half of the ring fail (e.g. fibre break) the traffic will be routed to its destination via the other half of the ring.

VODAFONE (NMC) have a network management centre that monitor and control their network 24 hours per day, 365 days per year. In the event of a fault being detected the appropriate maintenance team is despatched to rectify the problem in the shortest possible contracted timeframe.

The VODAFONE network has been configured such that all POA calls have two routes (primary and secondary) between VODAFONE switches, hence if one route is temporarily congested the call will automatically route via the second choice.

4.2.9.2 Transaction Network Services (TNS)

TNS provide two X25 link network links, one from IRE11, and one from IRE19, to HMS(HSBC Merchant Service) for DCS online debit card transactions.

The online component uses Transaction Network Services (TNS) to provide the network connectivity between Horizon Online and HMS. The batch component uses ISDN to transfer reconciliation files between DCSM and HMS. The batch component will use Post Office Data Gateway (PODG) to transfer files via the Internet in the future.

The network connectivity comprises:

• X.25 between Horizon Online and TNS

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- TCP/IP between TNS and HMS

4.2.9.3 *Talktalk Business*

Talktalk Business provide connections to Post Office Branches as part of the ConnectDSL service operated by Fujitsu.

The Talktalk Network Operations Centre in Irlam, Manchester monitor and controls their network 24 hours per day, 365 days per year. In the event of a fault being detected the appropriate maintenance team is despatched to rectify the problem in the shortest possible contracted timeframe, working with Fujitsu NOC and Core ISP where required..

4.2.9.4 *EMC – Disk Storage Supplier*

EMC provide Fujitsu with very high capacity, highly resilient disk storage systems in IRE11 and IRE19. There are very high speed connections between the two data centres that allow the data replication to ensure data is not lost following a major incident at the primary site (IRE11). EMC provide their own monitoring of their disk system in both data centres which enables fast identification and resolution of failures.

Belfast Refresh is replacing EMC with ETERNUS storage. A large number of servers have already migrated as part of Release 10, DAT services will migrate during Release 11, and BRDB & NPS during Release 12. See section 0.7 changes expected.

4.2.10 Data Centre Operations Service

UNCONTROLLED IF PRINTED

FUJ00232658

The Data Centre Operations Service is responsible for:

- 24 hours by 365 days a year operation.
- The provision of all Data Centre operations, which includes, for example; all the agents, servers, and databases used to manage and support the Branch Infrastructure and HNG-X Central Infrastructure used to deliver the Business Capabilities and Support Facilities irrespective of technology platform or geographical location.
- The day to day management and operational control of the Data Centre environments located in the live Data Centre and the Disaster Recovery (DR) Data Centre applying ITIL best practice within these environments.
- The monitoring within each of the respective Data Centres to an agreed level.
- On-site operational support in order to identify / minimise interruptions to the HNG-X Services provided by Fujitsu Services.
- Running the live Data Centre in an active DR mode, with the DR Data Centre being used for testing. The live Data Centre (including the communications in and out of the building) is, in its own right, fully resilient. Business Continuity testing is completed during the week (Monday to Friday) for a maximum of two (2) weeks per year, during which operational testing will not take place at the DR Data Centre.
- The AP Client File Re-Send Service – this service component of the Data Centre Operations Service is described in Annex A of this document.
- The Post Office SAP Hosting Service
- The Data Centre Operations Service will implement a maintenance plan, which shall be shared with Post Office on request, for the calendar year covering testing of the following environmental elements:
- The Environmental Maintenance Services
- Configuration Management
- Capacity Management
- Failover to the DR Data Centre

UNCONTROLLED IF PRINTED

NB: Impact of Loss of Datacenter has been written in the SVMSDMPLA0002-HNGx Service Business Continuity Plan. See section 11.1 Impact & Risk Identification, Item numbers from 31 to 44.

4.2.11 Support Services

4.2.11.1 The System Management Centre (SMC)

The System Management Centre service is being provided by Fujitsu Consulting India from Bangalore, India (IND49). SMC DR site (IND46) is at Pune, India.

The SMC team's primary function is to monitor and manage the POA HNG-X infrastructure via Tivoli eventing, The team provides 24 hours shifted service, every day of the year.

4.2.11.2 POA Customer Service

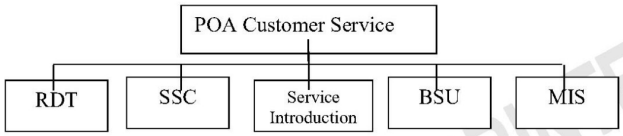
© Copyright Fujitsu Services Limited 2014

FUJ00232658

Fujitsu Services POA Customer Service support, operations and infrastructure services are provided primarily from the Fujitsu Services Bracknell (BRA01) building.

Fujitsu Services LEW02 has been designated the 'Disaster Recovery' site for the CS and essential Development support services which are provided from Bracknell.

The overall structure and functionality for contingency purposes may be represented as follows:



UNCONTROLLED IF PRINTED

4.2.11.2.1 Reference Data Team (RDT)

The Reference Data Team validates and processes live Reference Data in association with Post Office Limited at Chesterfield and the Post Office Limited Support Change Implementation Team who are also located in the Fujitsu Services BRA01 building. RDT validate changes whilst POL verify them.

The prerequisites to provide the service are:

Access to RDMS validation and verification counters; workstation access to live RDMS service;

Ability to receive Reference Data from, and send Reference Data to Post Office Limited at Chesterfield and BRA01 respectively (Also known as RDT team);

Access to Fujitsu Services (POA) infrastructure services i.e. E-mail, MIS, Peak, TRIOLE for Service, PVCS.

4.2.11.2.2 Third Line Support Services (SSC)

SSC provide 3rd line application support for the Horizon solution" and is available 24 hours per day, but is provided only on an on-call basis outside of 09:00hrs to 17:30hrs Monday to Friday, and Bank Holidays.

Horizon Online 3rd Line Application Support Service: Service Description in SVM/SDM/SD/0004

A support server for the SSC is located in IRE 11 (SSC). This platform provides the SSC with diagnostic information with the ability to access a three month archive.

The server is connected to the Data Centre host LANs and will be accessed from either

1. SSC Workstation PCs connected on a private LAN in BRA01, over an encrypted link to the Data centres using the firewall already installed and maintained in BRA01 by ISD.
2. From the SSN Servers in the Data centre

Access to SSN servers is limited to support staff only by use of two factor authentication. SSC staff have laptops dedicated to home use to ensure that they have an access route should corporate premises be unavailable in a DR situation.

SSC manage the PEAK call management system. See 6.11.2.2.2

In normal operations the SSC Support Server will be accessed in IRE11, however in a disaster recovery situation, the server may be started up in IRE19. Resilience is provided by the fact that the server resides in the BladeFrame environment.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

4.2.11.2.3 Reconciliation Service

The Reconciliation Service investigates and resolves all 'Reconciliation' incidents received from Post Office Limited.

The prerequisites to provide this service are access to the Business Incident Management (BIM) system, fax and telephone facilities.

4.2.11.2.4 Management Information Systems (MIS)

The Management Information Systems (MIS) function processes Management Information collected and processed on the DRS database and on the Data Warehouse.

The prerequisites to provide the service are:

Access from MIS Clients to the DRS and Data Warehouse databases, and to the MIS File server.

4.2.11.2.5 Service Introduction (SI)

Service introduction primarily consists of a Customer Service programme planning function and a Release Management function.

Release Management manage the release of software changes into the live environment across the Horizon and HNG-X service.

The prerequisites to provide the Release Management service are:

Access to Fujitsu Services (POA) infrastructure services i.e. E-mail, Peak, TRIOLE For Service, PVCS.

4.2.11.2.6 Change Control

The POA Programme Team manage two version control systems, PVCS and Dimensions.

PVCS is used for the Horizon Programme. To access PVCS users require either 'PVCS Terminal' or PVCS Dimensions PC Client.

Dimensions is used for the HNG-X programme. To access Dimensions users must first gain access credentials. Interfaces to Dimensions are then through a web interface or via the Dimensions Serena Client. Both require corporate LAN connectivity.

4.2.11.2.7 Configuration Management – Signing Server.

POA Programmes manage the day-to-day operations of the Configuration Management Signing server, which is used to authenticate software releases to the live estate. The primary CM Signing server resides in BRA01 and a secondary server resides in LEW02. The databases on these severs are synchronised on an hourly basis over the Fujitsu Services Corporate network. In addition daily back-ups are also taken of the Signing servers.

In the event of a disaster at BRA01 the Programme team can access the LEW02 CM Signing server using disaster recovery laptops at least one of which is held off site.

4.2.11.2.8 Live System Team

The Live System Test (LST) team, who reside within the POA Development organisation, test software changes about to be released into the live estate. This is achieved by proving the software changes on discrete test configurations that replicate the live software environment.

The prerequisites to provide this service are:

UNCONTROLLED IF PRINTED

FUJ00232658

- Availability of hardware test rigs upon which the live software set can be loaded and run;
- Access to Fujitsu Services (POA) infrastructure services i.e. Peak, TRIOLE For Service, PVCS, Dimensions.

4.2.11.2.9 Fourth Line Support

POA Development and the development teams of external suppliers provide the final line of support, generally referred to as fourth line support.

4.2.12 Operational Services sub-group

The Operational Services sub-group consists of the following teams:

- The System Operate Service
- Network Support
- POA Customer Support
- POA Programme and Development operational support teams.

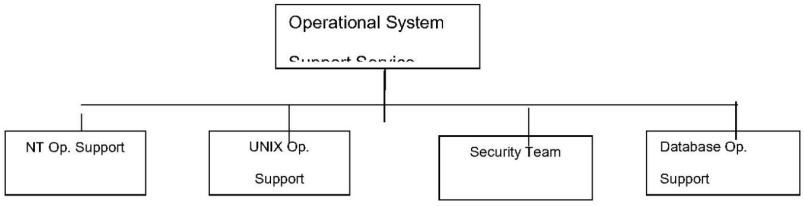
4.2.12.1 The Systems Operate Service

In providing an ongoing managed service for the Systems Operate, FSCS will provide POA with a support service covering the following areas:

- UNIX Support Service
- Database Support Service
- NT Support Service
- Systems Security Team

The overall structure and functionality for contingency purposes may be represented as follows for the Systems Operate Service (SOS):

UNCONTROLLED IF PRINTED



In providing the Operational Support Service FSCS provide POA with a round-the-clock service, managing and supporting those parts of the POA Solution housed in the POA Data Centres at IRE11 and IRE19. Below is a summary, which includes:

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- Management of the hardware maintenance.
- Management of the environmental controls.
- Management of the infrastructure maintenance to agreed schedules.
- Operate the service in 'supervisor' mode for special maintenance activities.
- Management and archiving of system and user filestore.
- Production and maintenance of archive reports.
- Production and maintenance of filestore repair tapes.
- Monitoring of the key service elements, to ensure that service issues are identified at the earliest possible opportunity.
- Responsibility for investigating all faults and problems arising on the Supported Systems, resolving the First Line support faults and problems, and where appropriate forwarding unresolved support issues to the FSCS or POA support teams responsible.
- Monitoring of the workflow through the Supported Databases. The Supported Databases will be automated via the Maestro scheduler but will be monitored by FSCS staff in IRE11. Any event, which cannot be resolved by first line staff, will be progressed to FSCS technical support.
- Provision of a duty manager, based in IRE11. The duty manager will act as a point of contact for POA and Post Office Limited operations staff for day-to-day operational dialogue and any escalation issues. A duty manager rota will be provided on agreed periodic basis.
- Monitoring the capacity usage of the Supported Systems and Operating System Software and advise POA when limits are being approached. FSCS will also provide recommendations on remedial action to POA.
- Management of off-site storage of system archives and recovery information.
- Collection of necessary diagnostics to allow faults to be progressed to resolution.
- Management of diagnostic links to subcontractors.

UNCONTROLLED IF PRINTED

4.2.12.1.1 UNIX System Support Service

The System Support Service will provide POA with comprehensive support for the Operating System Software from the FSCS Data Centre in IRE11 Belfast. This will include:

- Software support and system administration activities
- Investigation and progression of all system alerts and dumps.
- General housekeeping of the system error logs and audit files.
- Maintaining UNIX teleservice interfaces.
- Introduction of new hardware components.
- Applying changes to user and group security as necessary.
- Maintenance of file and directory permissions.
- Changing to communication cataloguing information as required.
- Maintenance of the network configuration information.
- Integrity checks on file systems and recovering inconsistencies as necessary.
- Responsibility for managing to a successful resolution, all problems and faults associated with the Supported Systems.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- Resolving of faults and problems arising on the Operating System Software.
- Ownership of the operations manual covering all aspects of the services provided as part of the Systems Operate Service.
- Management of the Supported Systems and Operating System Software.
- Management of ongoing operating system support activities
- Performing back-ups and recovering as necessary.

4.2.12.1.2 Database Support Service

The Database Support Service will provide POA with comprehensive support of the Supported Databases including user facing support activities from the FSCS Data Centre in IRE11 Belfast. Below is a summary, which includes:

- Database administration activities which include:
- The set up of users after a new software installation or upgrade.
- Exporting of data.
- Creation/recreation of databases.
- Upgrade, migration or creation of databases.
- Changes to the Supported Databases using Change Management.
- The import of data from an export as required in support of the Supported Databases.
- Installation and testing of build software after any change, upgrade of the operating system, upgrade of database software, or after modifications to the Supported Databases.
- Monitoring the Supported Databases using BMC Patrol and software supplier supplied views; run regular checks to monitor table-spaces, availability and fragmentation, and when appropriate reorganise the database (where reorganise includes: export, recreate and import).
- Management of problems and faults associated with the Supported Databases by forwarding calls resulting from the above support activities to the appropriate support unit.
- Investigation of faults and problems arising on the Operating System.
- Monitoring database utilisation and occupancy.
- Management of the Supported Databases under Change Management, recording software revision levels.
- Maintenance and administration of the Supported Database variables, under Change Management.

4.2.12.1.3 Windows NT / WINTEL Support Service

The Windows NT / WINTEL Support Service provides POA with comprehensive support for the Windows NT / WINTEL Software from the FSCS Data Centre in IRE11 Belfast. Below is a summary, which includes:

- Operating Software support and system administration activities for the Supported NT / WINTEL Systems as follows:
- Investigation and progression of all system alerts.
- Undertaking general housekeeping of the system error logs and audit files.
- Introducing new hardware components.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- Applying changes to user and group security as necessary.
- Maintaining file and directory permissions.
- Maintaining network configuration information.
- Performing integrity checks on file systems and recovering inconsistencies as necessary.
- Performing back-ups and recovering as necessary.
- Responsibility for managing to a successful resolution, all problems and faults associated with the Supported NT Systems.
- Management of the Supported NT Systems and Windows NT Software, recording software revision levels and hardware modification status in accordance with the FS POA Change Control Process.
- Install new releases of the Windows NT Software such that the minimum release levels for the software, as recommended by the software supplier, are correctly maintained.
- Provision of ongoing operating system support activities.

4.2.12.1.4 Systems Security Team

The installation and configuration of POA firewall systems including: IRE11 & IRE19, LEW02 and Bracknell. On each system, the Systems Security Team manage the UNIX hardware and operating system which includes users, file-systems, system backups and installed applications e.g. Checkpoint Firewall-1. The configuration of Checkpoint Firewall-1 rule bases is managed by the Network team.

4.2.12.2 Network Support Services

The Network Support Service based at WAR07 provides POA with comprehensive support for all aspects of the Live POA Network and limited support of POA related test networks. The network service is provided by the Network Support team. The service includes:

- Support 24 by 7 for operations and network services.
- Investigation of all network related issues to 3rd line and progression and monitoring of those calls that go to 4th line support organisations.
- Progression and monitoring of WAN/ISDN and network hardware issues for non-Live POA related test environments that require 4th line support assistance.
- Monitoring of all network and some host elements of the live service using HP Openview as required.
- Maintenance and support of all network hardware on the live estate.
- Management of Network hardware systems connected with the live service at remote sites.
- Management of IP address schemes and databases at all sites connected with the live service.
- Management of the Network cable infrastructure and databases in IRE 11 and IRE19 Data-centres.
- Management of cable infrastructure at all Live remotes sites.
- Introducing new network hardware or configuration elements.

4.2.13 The Major Account Controllers (MAC)

4.2.13.1 Overview

Major Account Controllers (MAC)

UNCONTROLLED IF PRINTED

FUJ00232658

MAC team are responsible for managing/owning Incidents between 08.00 and 20.00

Monday to Friday, 08.00 to 17.00 Saturday and Bank Holidays 0800 – 1400 excluding Christmas

Day. The MAC team also manages the incident transfers to the Atos Service Desk for issues in POL Clients domains. The SMC assume this responsibility out of hours, i.e., outside these hours. The SMC are responsible for escalation of incidents to the POA OOH Duty Manager.

1. **Communications Management Team (CMT)**

   This team manage network issues with third party e.g., BT.

2. **Management Information Team (MIS)**

   This team provides internal and customer reporting and also measures all SLAs, both contractually and internally.

TRIOLE for SERVICE (TfS) is used by the MAC and SMC teams as an incident management system, and by POA as a Problem Management system. These services are provided from a shared location at either SDC01 or SDC02.

UNCONTROLLED IF PRINTED

4.2.13.2 Communications Management Team (CMT)

The CMT service complements the ATOS.

- The CMT Service is available from 08:00hrs to 17:30hrs Monday to Friday and 08:00hrs to 12:00hrs on Saturdays and bank holidays (excluding Christmas Day)
- The CMT is a function responsible for providing an end-to-end management to resolution of all network related incidents which render the service unavailable within the Branch.
- The CMT provides an enhanced level of value add activity to maximise the speed at which network related incidents are resolved and the service restored to the Branch. As part of this approach, both Post Office and the Branch are informed at regular intervals as to the status of the incident.
- The CMT will input into, the Daily Report provided by Fujitsu Services to Post Office which identifies all Branches with open incidents and the current status of those incidents. This daily report enables Fujitsu Services and Post Office to track and monitor the progress of incidents and escalate any specific problems to minimise the amount of time the Branch cannot trade.
- To ensure the Branch and Counter Position availability is kept to a maximum and within the Branch and Counter Availability Service Level Targets (SLT), the CMT will work closely with the Systems Management Service. Where an event or a system or network incident has been identified, the Systems Management Service will raise an appropriate incident, (this may be in advance of any incident raised by the Branch), at the required severity / priority level to enable the issue to be resolved

4.2.13.3 Major Account Controllers (MAC)

The MAC team will be a link between Fujitsu Services and the Atos Service Desk.

MAC team hours of cover is 0800 to 2000 Monday to Friday, 0800 to 1700 Saturdays and 0800 to 1400 on Bank Holidays excluding Christmas Day.

The team's email address is MAC GRO – Emails will be acknowledged within 1hour of receiving

Telephone Number GRO

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Overview of their General Tasks -

- Global User Reset and unlocking of Passwords for Postmaster's and POL employee's –
  - 30 minutes response time
- Single point of contact for Atos Enquiries and Escalations
- Engineering Priority 1 Incidents which have failed SLA
- Engineering Priority 3 Incidents which have failed SLA
- High Priority Incidents, Horizon System Failure
- POL/PM escalations on incidents within the Fujitsu Domain which have failed SLA
- File Transfers
- Engineering or Network Customer complaints which require a Fujitsu response
- Engineering Cancellations

4.2.13.4 *Electrical Power*

To provide contingency against mains power failure, the TfS system is covered by UPS and generators in SDC01, and the telephone communications equipment in STE04 is also covered by a UPS and standby generator. In the event of power loss at either of these locations it is expected that continuous power is provided, initially by the Un-interruptible Power Supplies and then by the generators.

UNCONTROLLED IF PRINTED

4.2.14 The Message Broadcast Service (MBS)

- The Message Broadcast Service enables Post Office to communicate directly with Branches, for the purposes of issuing instructions, advice or information urgently, where paper and postal communications may be too slow or inappropriate. The Message Broadcast Service only enables communications from Post Office out to Branches; Branches are unable to respond or communicate to Post Office using this Service.
- Each Message is distributed to target Branches as identified by Post Office.
- Only Branches that are currently in communication with the HNG-X Central Infrastructure at the time of the Message Broadcast will be able to access the Message.
- Messages approved for distribution to the Branch Infrastructure are distributed by the Reference Data Management Service on behalf of the Message Broadcast Service.

4.2.14.1 *Service Availability*

The Message Broadcast Service is available during the hours of: 08:00hrs to 20:00hrs, Monday to Saturday, excluding all Bank Holidays. In exceptional circumstances, Post Office and Fujitsu Services may agree to distribute a Message outside of these hours.

- The loss of both the Data Centre Operations Service and the Reference Data Management Service would affect the ability of the Message Broadcast Service to issue a Message Broadcast.

4.2.15 Service Integration Service

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The Service Integration Service is provided by Fujitsu Services to allow for services to be provided on non HNG-X Service Infrastructure and to be delivered alongside the HNG-X Service Infrastructure.

The Service Integration Service will be available from 9:00hrs to 17:30hrs Monday to Friday excluding Bank Holidays or at other specific times agreed.

4.2.16 Receipt Template Service

The Receipt Template service is provided as an extension to Operational Business Change and does not, in itself, provide any 'Live' service, and consists of a single component, namely the provision of new or amended templates to be applied to Automated Payment receipts on the HNG-X system.

The primary elements of this service is to cover the receipt, production and verification of new, or amendments to existing, receipt templates.

Within the context of this service there are three types of change:

- New – where the template does not currently exist
- Major amendment – where the structure or flow of an existing template is being changed
- Minor amendment – where the amendment to an existing template is not to structure or flow, e.g. change of text

Within the context of these types of changes, the content of a Receipt Template is restricted to the underlying functions which are available at the time that the new/amended template is requested. If Post Office requests a template where the underlying function is not currently available Fujitsu Services will inform them that this is the case and Post Office will then raise a Change Request in order to have the new functionality added to the receipt template mechanisms.

See SVM/SDM/SD/0022 for more details

4.2.17 Service Management Service

4.2.17.1 Service Elements

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- the provision of monthly service reports;
- the management of the HNG-X Services other than the BCSF Services in their achievement of all SLTs, Operational Level Targets (OLTs), performance metrics and design targets;
- the management of service improvement plans in collaboration with the Post Office;
- the liaison with Post Office in respect of the overall performance of services;
- all aspects of Data Centre operations availability management, network management, systems management and technical interfaces with Post Office Clients and other domains; and
- the maintenance and management of Business Continuity Plans
- Problem Management
- Branch Issues Management
- Complaints Procedure
- Service Improvement
- Operational Change Proposals
- Configuration Management

All elements of the Service Management Service are provided from Bracknell (BRA01) and are available Monday-Friday 09:00hrs -17:30hrs excluding Bank Holidays, with the following exceptions:

- release introduction activities such as Data Centre migration or Software distribution will be carried out in accordance with relevant project plans; and
- duty management is available 24 hours a day, every day of the year.

See SVM/SDM/SD/0007 for more details of the service, and the POA Organisation Chart for the structure of the POA Service Delivery team.

UNCONTROLLED IF PRINTED

4.2.17.2 Loss of primary operational office site in Bracknell

Provision has been made for staff to either work from home or to relocate to the DR site at LEW02.

4.2.18 Internet Data Exchange (DXI)

This service provides the Internet DMZ. The Internet Services Hub provides for outgoing connections only (server initiated towards Internet). The services identified within the service hub are:

FUJ00232658

- MGRM to MoneyGram Intl. test service (http)
- BKAC Agent - validates Bank Sort Code and Account Number. A Web Service Agent implemented in the TWS that interacts with the BACS Checker Service (http)
- BACS Checker Service Postcode Anyware - A Web Application provided by Postcode Anywhere for validating Bank Sort Codes and Bank Account Numbers. (https)
- BBND Agent - A Web Service Agent implemented in the TWS that interacts with the ADSL Checker Service. (https).
- PGDD to Neopost's Bank Guaranteed Delivery Calculator (SOAP over http), called Kahala. Neopost calculates a GDD for delivery from one postal location to another. A Web Service Agent implemented in the TWS that interacts with the GDD Calculator Service Application
- SSL VPN traffic from HNG-X to EMC addresses (https).
- EMC Remote Support Gateway (RSG).

This is a single non-resilient Internet access service through each data centre (IRE11 and IRE19). Although non-resilient, redundancy of access between sites is provided and services can be manually restored between sites.

4.2.19 Corporate Data Exchange (DXC)

DXC is a platform and applications that facilitates the transfer of material between the HPEV (HNG-X production environment) and the FSEV (Fujitsu Services corporate environment); it will act as a barrier to protect HPEV from corporate network based threats and vice versa and will provide mechanisms to:

- Control the transfer of data between the HPEV and the FSEV and vice-versa.
- Audit to ensure that any material moved between the two environments is identified and an appropriately granular record is made.
- Maintain access and control policies.
- Provide procedural control mechanisms on the transfer of such data.

The operating system is Secure Red Hat Linux.

The Database Server is PostgreSQL.

It will accept only data from agreed databases/schemas in an agreed format; there will be no facility to perform undefined transfers. Transfers may be scheduled or unscheduled (ad-hoc in JSCAPE terminology).

The Web Server is the web transfer component of JSCAPE Secure FTP Server.

The file server is JSCAPE Secure File Server complemented by JSCAPE Secure FTP Factory, complemented by bespoke clients' written using JSCAPE Secure FTP Factory.

Since JSCAPE will be managing both types of data transfer, there will be single, managed mechanism for control, logging and reporting.

A virus and malware checker is supplied which vets all material transferred to HPEV.

Availability

UNCONTROLLED IF PRINTED

FUJ00232658

This device will be in a live/standby configuration with the equivalent platform at the DR site. It will be provisioned on a blade or vBlade with a recovery time of 15 minutes or less.

Network Topology

The server will be placed in a network topology indicated by "DXC Corporate Data Exchange Proxy" as shown in the diagram below.

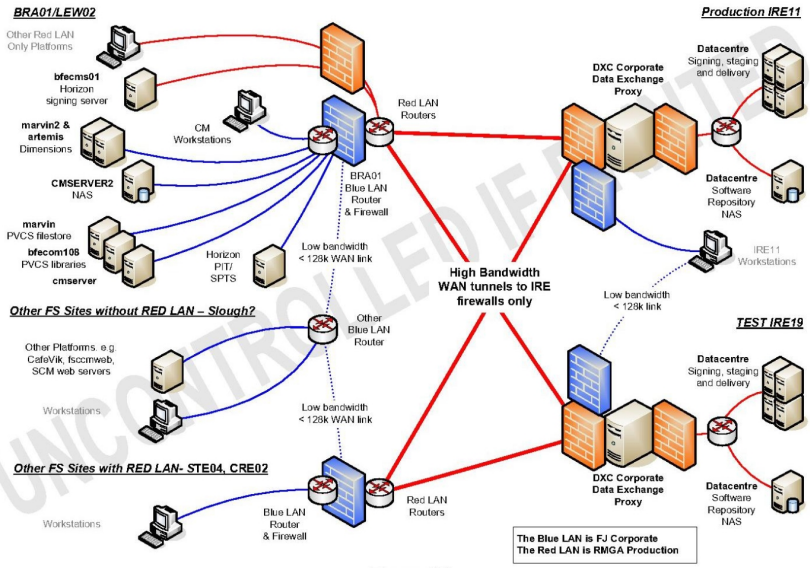


Figure 28

Network Topology

4.2.20 Performance & Capacity Management (SPN)

The Capacity Database is an essential part of providing an effective capacity management function to the Post Office Account. The role of the database is to provide a central repository for system and selected business metrics which can be interrogated to provide a picture on the current performance of essential services and can be extrapolated or modelled to provide a view of the near future.

The performance database is required to store data relating to service metrics. These will include metrics related to Operating System, Middleware, Database, Applications (bespoke and COTS), API's and Defined Service Levels. These metrics are used to build a picture of the performance of a system and can assist in the resolution of performance as well as availability issues.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

There are two main access methods to this server for management purposes:

- TCP/IP level access provided by the Secure Access Server
- HTTP / SQL access via the Corporate Data Exchange Proxy solution.

This provides the means by which the System Qualities and other support teams can access and manage the SPN platform.

An SPN platform instance is present in both datacentres in an active / passive configuration. The disks are provided by Clariion storage and make use of replication to ensure synchronicity of data between both frames.

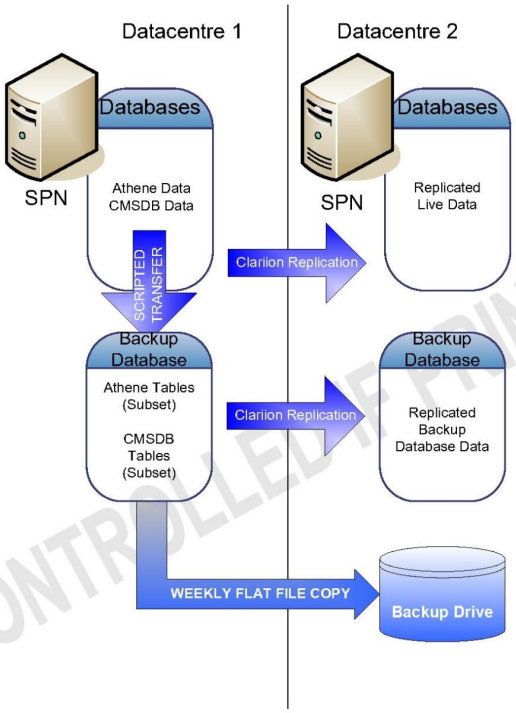
The solution is based on SAN-Attached hardware and therefore is inherently resilient against disk failures given the RAID architecture employed by the EMC Clariion system.

To ensure high availability, the disks are synchronised with the passive data centre. This ensures that in the event of a disaster scenario, the system qualities team can continue to capture and collect system performance data.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658



UNCONTROLLED IF PRINTED

Figure 29

4.2.21 Branch Support Database System (BRSS)

4.2.21.1 Overview

The Branch Support Database (BRSS) system provides a dedicated, available and resilient (as it resides within BladeFrame) repository of Live transactional, reporting and control data for the various HNG-X business and technical support streams to provide levels of support to the Post Office Branches and Post Office Limited.

The BRSS system runs on a single p-blade within the Fujitsu-Siemens' BladeFrame environment using a SAN-based storage solution (BRS – Branch Support Server).

The Branch Support Database is implemented in the form of a single instance Oracle Enterprise Edition database.

The BRSS transactional repository consists of the following type of transactional, reporting and control data:

- **User and Session Management**

  Counter users, roles (Clerk, Manager etc) and stock units.

  log-on/log-off events and session establishment.

FUJ00232658

(Migration specific) Outlet migration status

- **Audit**

  Auditable requests

- **Settlement Basket Capture**

  Settlement transactions.

- **Reporting**

  Transaction level and aggregated report data.

  Report generation requests (events) used for audit and reporting purposes.

- **External Authorisation Transaction Recovery**

  Control information for recoverable transactions.

- **Track & Trace**

- **Counter Reference Data**

- **Cash and Stock Pouch Despatches, Advice Notices**

- **Delivery & Collection Notifications and Cash Declarations**

- **Message Broadcast (Desktop Memo)**

UNCONTROLLED IF PRINTED

Data in the Counter audit store is retained for 14 business days.

The data in Transactional, Recovery, LFS and Track & Trace tables is kept for up to two months (sixty two calendar days).

Data in the Reporting transactional and aggregation tables will be retained for six months (182 calendar days). All control and metadata tables are based on the same retention period of 182 calendar days.

The BRSS system consists of a number of Linux-based host processes that are run by scheduling software. These processes typically perform operations such as table & index partition management, consuming data replicated from the Branch Database and file / table housekeeping.

BRSS runs in archived redo-log mode to provide the facility of point in time recovery. RMAN will be used as the tool for performing backups and restore/recovery.

4.2.21.2 Data Population

FUJ00232658

The Branch Support Database (BRSS) contains transactional, event and other relevant data replicated from the Branch Database. For the customers (technical / business support streams) to be able to use BRSS as the sole point of access to live data, relevant data is replicated to BRSS on a near real-time basis.

4.2.21.3 *Support Interface*

The Branch Support Database is the first point of call for any support queries related to Branch information.

All applications run under the batch scheduler through defined Unix users with only the necessary access to run the application.

Oracle database connectivity and access control is through defined Oracle Users and the Roles granted to those Users would only be those that are necessary to run the application.

Data security is maintained by constraining the database object by type and range and by restricting access through Role to only those applications requiring such access.

Note that the BRSS is used for all support queries that are run by the support teams. The only circumstances under which the Branch Database can be used for querying data instead of the BRSS is:

- The Branch Support System (BRSS) is down / inaccessible or the replication between the Branch Database and Branch Support System is down / or too far behind.

4.2.21.4 *Resilience / Fail-over*

The Branch Support Database runs on the BladeFrame Linux environment. Fail-over is implemented using a remotely mirrored EMC file store while resilience to hardware faults can be handled by the BladeFrame technology's inherent fault management and resolution.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

5 Testing Strategy

5.1 Initial Testing

The initial testing of all business continuity contingency plans has been documented in the HNG-X Business Continuity Operational Test Plan (SVM/SDM/PLA/0003).

Some tests are focused at sub-service level, however other tests are based upon a facility, e.g. the Loss of a Data Centre (IRE11).

5.2 Ongoing Test Strategy

This refers to how the contingency measures, in place for the HNG-X Support Services, shall be periodically tested to ensure they are current and reflect the service model for those services as they mature.

This is provided by an ongoing series of business continuity tests at a predetermined frequency for the duration of the Fujitsu Services POA contract. The nature of these tests is documented in the HNG-X Business Continuity Operational Test Plan (SVM/SDM/PLA/0003), which also contains a yearly test schedule.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6 Preventative Measures

It is a fundamental philosophy of the POA solution that wherever technically possible, components of the service are designed in such a way as to ensure maximum resilience to failure by way of eliminating possible single points of failure, i.e. by providing multiple platforms performing similar functionality both for performance and resilience.

In general HNG-X provides resilience based on the installation of an additional server (whether physical or virtual) over and above that required for normal operation. These additional servers are located in the primary data centre in IRE11.

For example The Key Management Service (KMN) only requires one server to perform all normal tasks, however there are two servers in IRE11 creating an N+1 implementation (where N is the number of servers required for normal operation). In addition, since the KMN server is hosted on a bladeframe, there is extra resilience via a spare blade in the same cabinet which can be used as a direct hardware replacement should the designated hardware fail.

6.1 Major Account Controllers (MAC) DR facility

The Major Account Controllers (MAC) service can be delivered from the Disaster Recovery site in BRA01 following a relocation of staff from Stevenage. The relocation can be completed within around 3 hours of the decision to enable the DR site. POA staff in Bracknell would assist with the initial setup activities.

6.2 Triole for Service (TfS) – Service Desk system

Should the primary Incident Management System (TfS) sustain a total failure there is a second system that is kept updated in SDC02 which can be brought into use.

6.3 Data Centre Operations Services (IRE11 / IRE19)

The HNG-X service is based upon using the two Data Centres (IRE11 and IRE19) at the same time for live services, the primary Data Centre being IRE11. In normal operational mode IRE19 is supporting the live service while also accommodating the test environment for HNG-X.

- Both Data Centres operate 7D x 24H x 365/366 days with operational staff on site at all times. The sites are located approximately 5 miles apart (11 miles by road).

In a situation where IRE19 is unavailable then a full live service can be provided through IRE11.

However, if IRE11 (the primary site) becomes unavailable then a full service can be provided from IRE19 only following a full site failover. It is expected that all test and development facilities services will be unavailable while running a full live service from IRE19, however there may be provision for a limited test service.

The overall HNG-X solution adopts and demonstrates industry best practice in areas such as systems enterprise and operational management.

This provides the capability to monitor and report on virtually every hardware component and software application comprising the HNG-X solution.

It also allows a significant amount of automation to be introduced into the overall HNG-X capability, which in most situations allows timely resolution of any failures that are experienced.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The impact of loss of datacenter have written in SVMSDMPLA0002- HNGX services business continuity plan, in section 11.2 , Item number 31 to 44.

6.3.1 Environment Monitoring Facilities

IRE11 & IRE19 Operations staff monitor the environmental facilities against potential threats.

Examples would be:

Loss of mains power	UPS and Generator take on load
Loss of Air Con	Standby unit brought into use
Flood / Fire warnings	Detection systems will give early warning

Early detection is the key to the preparedness, the building disaster detection facilities are regular tested and appropriately maintenance in accordance with contractual agreements. In the event a problem is detected, which may affect the live service kit, the appropriate support group responsible for implementation of fault resolution or instigation of disaster recovery will be immediately contacted.

FSCS has a comprehensive maintenance and call out contract, covering all environmental kit. All contractors are on a 4 hours response to site basis agreement, and since resilience is built into the main systems, only minor disruption should occur.

See Appendix 2 (IRE11) and Appendix 3 (IRE19) for further details.

UNCONTROLLED IF PRINTED

6.3.2 Data Centre Air Conditioning – IRE11 & IRE19

- Both IRE11 Tech Halls are served by six air conditioning units. The environment can tolerate the loss of two of these units without impact.

  Portable units are also available in the case of emergencies.

- The IRE19 Tech halls are served by eleven air conditioning units.

  The loss of a single unit within any of the halls would require addressing in the form of arranging for a portable unit to be obtained.

6.3.3 Data Centre Power – IRE11 & IRE19

- The Primary Site is at IRE11.

  This has two feeds from independent substations to onsite transformers. The site is capable of running for three days at peak load when on generator power, or longer provided fuel deliveries to site are possible. IRE11 has two computer rooms (or Tech Halls) which are physically separate buildings. TH2 is the site for the majority of the HNG-X equipment, and is fully N+1 resilient for UPS and generator power. TH1 is connected via separate paths of single-mode and multi-mode fibre-optic to allow the use of a row of cabinets for POA equipment. TH1 has N+1 resilience in UPS, but only a single generator.

  In practice the double failure of NIE supply and generator is highly unlikely, and there is a programme of generator and UPS testing each year to ensure that the generator is serviceable.

  Further information for IRE11 is outlined in the Appendix.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- The Secondary Site is at IRE19.

  This has a feed from a single substation with the transformer offsite. The site is capable of running for eleven days at peak load when on generator power.

  Further information for IRE19 is outlined in the Appendix.

Neither site shares a common substation and Northern Ireland is a resilient part of the National Grid with inter-connectors to Scotland and England.

At both sites: power is supplied to each server rack / equipment from a single / triple breaker via armoured cable fitted with commando socket and plug in the floor void to the equipment.

Power is routed to each piece of equipment via separate PDUs unless single source power. Power can be isolated via either the breaker within the PDU or switch on the commando socket. New suppliers can be upgraded or downgrade by replacing the breaker within the PDU.

UNCONTROLLED IF PRINTED

6.3.4 Oracle Real Application Cluster (RAC)

The Branch Database and the NPS database both use Oracle Real Application Cluster to provide high availability.

This configuration provides load balancing of client requests during normal operation. Additionally, if one node in the RAC cluster fails the other nodes takes over the load.

Therefore, the system capacity is managed in an N+1 configuration, such that the RAC cluster can handle peak load even with one failed node.

Branch Database N=3 (four nodes normally active)

NPS N=1 (two nodes normally active).

For Branch Database each branch will normally access the same node, if a node is unavailable then the failed node's branches is spread across the remaining nodes.

NPS supports several services e.g. ETS, DCS, NBS as if they were separate applications. A branch connection goes to the same node for any one of these services, but the branch does not necessarily use the same node for all services.

6.3.5 Oracle DataGuard

Oracle DataGuard is an Oracle feature which allows one or more standby databases to be maintained in a transactionally consistent fashion to a primary database. This is achieved by applying changes from the primary database to a secondary copy of the database.

The production Branch Database is the primary database, and a secondary copy of this database is maintained at the same site. The purpose of this secondary database is to guard against physical corruption of the primary production database, i.e. some form of unrecoverable I/O error resulting in a loss of database integrity.

Because of the manner in which the changes are propagated at application level, applied changes it is very unlikely that a data corruption will be propagated, and in the event of the primary being unavailable due to a corrupt block failover to the standby is extremely fast. The primary can then be repaired.

6.3.6 Disk Storage Arrays

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Both the Symmetrix and Clariion storage arrays have a high level of internal resilience.

Storage arrays are provided with power from separate Data Centre power supplies, and these are themselves supplied through independent uninterruptible power supplies and separate breaker (fuse) panels. Internally the storage arrays have many features the mean that failure of a single component is unlikely to affect the ability of the array to continue offering a service.

Within individual disk arrays RAID is used to ensure data integrity in spite of the loss of a disk drive (either a RAID-1 mirror or RAID-5 parity stripe).

The disk arrays also allow point-in-time copies of data to be maintained as snapshots or cloned copies. These enable rapid recovery from corruption.

Belfast Refresh is replacing EMC with ETERNUS storage. A large number of servers have already migrated as part of Release 10, DAT services will migrate during Release 11, and BRDB & NPS during Release 12. See section 0.7 changes expected.

UNCONTROLLED IF PRINTED

6.3.7 SAN Fabric

The SAN Fabric is built around two fibre-channel switches (directors) at each Data Centre. The two switches are independent, that is, they form two separate SAN fabrics.

This provides at least two forms of redundancy – firstly, the two fabrics allow for failure of any element in any one fabric (assuming both server and storage are connected to both fabrics). Secondly, a (human) error during a configuration change on one fabric will not affect the other independent fabric, typically allowing the change to be corrected before any adverse results are encountered.

6.3.8 Host Systems

All systems that connect to the storage arrays have two HBAs, each HBA connects to a different FC director, and therefore to a separate fabric. Multi-pathing is managed either by the control blades in the BladeFrame, or by host based multi-pathing for the relevant platform.

If one of the Storage ports, HBAs or FC directors fails or if there is a cabling problem, it will not cause the server to lose its connection to the storage.

6.3.9 Blade Frame and Storage Overview

HNG-X storage is synchronously replicated between the Live and DR data-centres using SDRF via the Intercampus link described earlier. Before a write is acknowledged to a server, it is written to the storage at both data-centres to ensure consistency of data between the sites.

The Symmetrix DMX disk arrays are operated as two independent pairs. One will contain the Branch Database, and the other the Branch Standby DataGuard copy. In the unlikely event that a fault develops with the storage continuity of service is ensured, as at least one copy of the Branch Database will be available.

The CX3-80 Clariion also supports an area of disk for Oracle RMAN backup. This is the primary recovery point for Branch Database corruption, and online storage is provided to allow recovery to be made in as timely a manner as possible. The Storage Area Network for HNG-X is illustrated in Figure 30 below

© Copyright Fujitsu Services Limited 2014

FUJ00232658

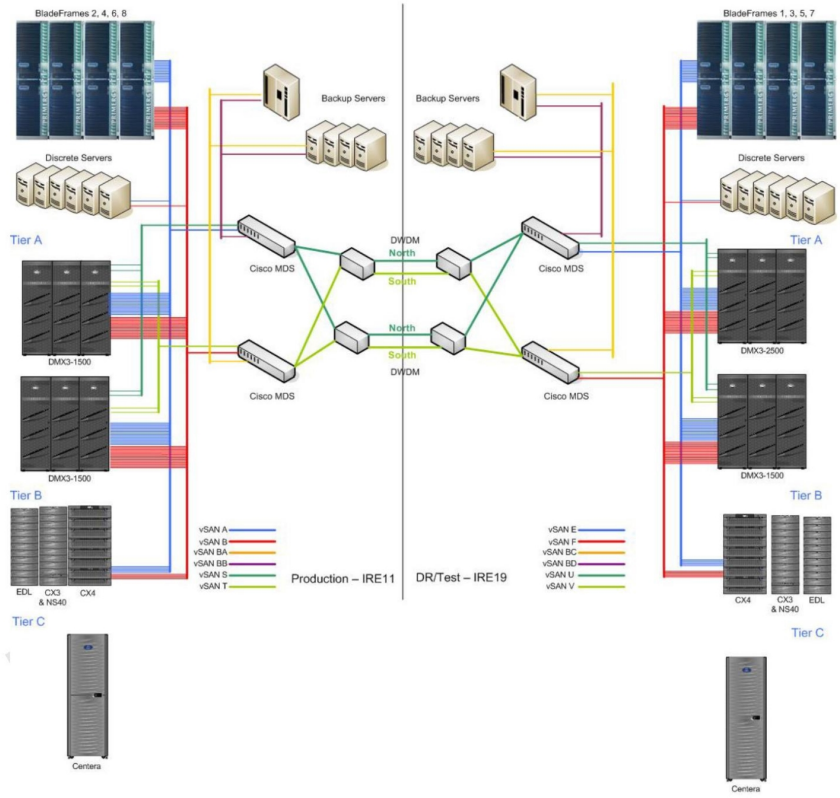


Figure 30

The BladeFrame system introduces the concept of a stateless server. Within the BladeFrame the actual processing unit only contains CPU and memory. All other components that usually make up a server are abstracted and provided by the BladeFrame chassis, e.g. network interface cards and host bus adapters.

The storage subsystem is external to the BladeFrame system and no HNG-X server hosted inside the BladeFrame has internal hard drives or other storage devices. A server is defined as a combination of a blade with a CPU and memory with resources such as a network interface, a host bus adapter and a storage subsystem. This configuration is held in a XML file. As a consequence the definition of a server (or platform) can be moved from one physical blade to another, from one BladeFrame to another or even from one data-centre to another.

BladeFrame from Fujitsu-Siemens consists of a chassis with up to 24 stateless processing blades (pBlades), two control blades (cBlade) and two switch blades (sBlade) in a cabinet with a foot-print similar to a normal server cabinet.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Please refer to the Platform Hardware Instance List, DEV/GEN/SPE/0007, for the latest configuration of the HNG-X live environment in IRE11 and test environment in IRE19.

The application of the BladeFrame technology for the purpose of disaster recovery to the HNG-X solution enables the meeting of the SLT for CAPO and all other HNG-X services. A farm of three BladeFrame systems is installed in each of the HNG-X data-centres.

The BladeFrame farms are composed of identical hardware in both data-centres. The configuration of the Live farm is captured in a configuration file. This configuration file is replicated to the DR data-centre at regular intervals. All data and operating system information that is held in the Live data-centre storage arrays is also replicated to the DR data-centre according to predefined criteria (either synchronously or asynchronously).

In the event of a disaster the configuration of the Live BladeFrame farm is applied to the DR farm. This process configures the DR farm identically to the unavailable Live farm and then presents the replicated Live data to the farm. This process has been designed to complete in less than an hour allowing for time for UNIX Support to check that all applications and services are ready to go Live again, enabling the branches to trade.

UNCONTROLLED IF PRINTED

6.3.10 BladeFrame Connections

All server instances on BladeFrame reside on the Core switches, and the BladeFrame is not physically connected to the Access switches.

It is necessary to distinguish between the management interface, which is a single connection to each cBlade, and the network ports available for pServer instances. Each BladeFrame will attach on cBlade to the header and one to the footer. For out of band support an Aurora Console Tower system (CON) will be provided that allows secure, managed serial connections to the serial port on the control blade.

Each BladeFrame has two management ports, one on each cBlade, and these are connected to different Data Centre switches. The PAN Manager service has a virtual IP which fails over to the master cBlade. The cBlades provide proxy arp resolution for each other, and simple ping tests are an unreliable way of tracing network problems.

Each cBlade has four on-board and four PCI based gigabit NIC for use by the pServers. These are grouped into resilient Ethernet interfaces (rEth) which may also span BladeFrame chassis as mega-rEth (mrEth) if a BladeFarm has been formed to allow a pServer to move between chassis.

Virtual switches are created within the PAN, and these are identified with the NIC that traffic is passing through and the security domain of the VLAN ID, e.g. vSwitch1_DB or vSwitch15_SAS. The LPAN Administrator will ensure that servers are only permitted access to those switches associated with VLANs in which that server resides. The PAN Administrator ensures that Test VLANs are not visible to Production systems and vice-versa.

6.3.11 BX900/PAN7

There is one radical change in architecture from PAN5, which is that the storage path is now "native" to the BX900 chassis, and does not pass through the PAN Ops management servers. This allows a pair of relatively small RX200/S7 servers to run as a cluster providing PAN Manager services, managing up to 16 BX900 chassis, each containing up to 18 "pNodes", as the BX924/S3 blades are now known.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Each BX900 has a clustered pair of management blades and an active/active pair of connection blades. For PAN7 these are Brocade VDX2730 switches capable of Ethernet or Fibrechannel connectivity. The pNodes themselves have a common network adapter (CNA) very similar to the current pBlades, with the connection blade taking the place of the sBlade and cBlade in a Bladeframe, and the internal connections of the BX900 taking the place of the Bladeframe backplane.

Currently extended control is provided through a ServerView VIOM server, but a later release is expected to manage the BX900 directly.

R12 will only migrate the RAC clusters, which are currently deployed as "bare metal" pServers. An initial installation of Oracle Virtual Machine (OVM) as a hypervisor will permit the RDT RLS servers to be deployed virtually.

It is expected that a later release of PAN7 will provide vBlade type functionality, but details are not yet clear, and the only virtualisation currently supported by Oracle is OVM.

An overview of the failover mechanics are shown in the figures below, but the principle follows that used in Bladeframe/PAN7, that the PRoduction LPAN is created and started on the DR hardware.

PAN7 provides a more extensive suite of tools for importing LPANs from a DR archive, simplifying a process that had been written as part of DEV/INF/LLD/0066.

The essential precursor steps of storage and network failover are still required.

The storage is presented to the individual pNodes rather than to the cBlade. Although this makes more work for the storage management team storage discover via SMIS makes the PAN Admin task very straightforward, and it is easy to manage small sets of LUNs in ETERNUS LUN Groups for each server rather than the huge presentations that had to be managed for Bladeframe

CONTROLLED IF PRINTED

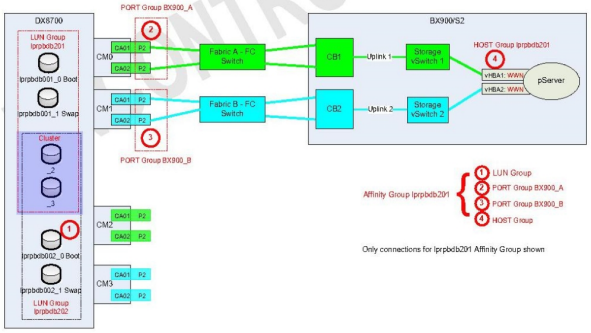


Figure 31

6.3.12 Salesforce Support Service

The Salesforce Support Service provides Post Office with a hosted and managed service for the PerspecSYS data residency solution (to host software as procured directly by Post Office). Support desk services will be provided to log calls from Post Office's end user help desk for issues relating to the hosted service and the Salesforce solution instances used by Financial Specialists and Stakeholder Management teams.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

The Fujitsu Salesforce Support Service(SVM/SDM/SD/1977) provides hosting, support, and service management for the PerspecSYS data residency solution which forms a critical supporting technical service for the Post Office Finance Specialists Salesforce Solution.

The Fujitsu Salesforce Support Service also provides call logging and incident routing for technical problems encountered by Finance Specialists and Stakeholder Management.

RESPONSIBILITY SUMMARY:

	End User Viewpoint	
Area of responsibility	**Finance Specialists Salesforce Solution**	**Stakeholder Management Salesforce Solution**
End User Help Desk	Post Office	Post Office
Call Logging and Incident Routing for technical faults	Fujitsu	Fujitsu
Resolving hosting and connectivity issues related to the PerspecSYS software	Fujitsu	Not applicable to Stakeholder Management Salesforce Solution
Service management for the hosting and support of the PerspecSYS software	Fujitsu	Not applicable to Stakeholder Management Salesforce Solution
Resolving application software issues related to PerspecSYS software	Post Office (PerspecSYS contracted to Post Office) Fujitsu will route the incident to the PerspecSYS support team and notify Post Office End User Help Desk	Not applicable to Stakeholder Management Salesforce Solution
Resolving Salesforce technical issues	Post Office has the direct relationship with Salesforce and Fujitsu is not providing an End to End Salesforce service. Fujitsu will take calls and resolve the issue when the problem originates in its own domain, however where the problem has not originated in the Fujitsu domain Fujitsu will pass the call to Post Office End User Help Desk who are responsible for raising calls with the Salesforce support team. Additionally Fujitsu will take and manage the resolution of calls raised with Salesforce	Post Office has the direct relationship with Salesforce and Fujitsu is not providing an End to End Salesforce service. Fujitsu will take calls and resolve the issue when the problem originates in its own domain, however where the problem has not originated in the Fujitsu domain Fujitsu will pass the call to Post Office End User Help Desk who are responsible for raising calls with the Salesforce support team. Additionally Fujitsu will take and manage the resolution of calls raised with Salesforce that breach the SLA target that exists

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	that breach the SLA target that exists between Post Office and Salesforce. These Salesforce Support Service Escalated Calls will be chargeable under a separate monthly fixed charge that will be reviewed after the first three months of live service.	between Post Office and Salesforce. These Salesforce Support Service Escalated Calls will be chargeable under a separate monthly fixed charge that will be reviewed after the first three months of live service.
Resolving Post Office communications network issues	Post Office (via communications network supplier) If the call is initially passed to Fujitsu by the Post Office End User Help Desk it will be passed back so that a call can be raised by Post Office on the communications network supplier	Post Office (via communications network supplier) If the call is initially passed to Fujitsu by the Post Office End User Help Desk it will be passed back so that a call can be raised by Post Office on the communications network supplier

UNCONTROLLED IF PRINTED

Service Availability:

The supported hours of operation for the Salesforce Support Service hours are 08.00hrs to 18.00hrs Monday to Friday and 08:00hrs to 12:00hrs on Saturday's excluding Bank Holidays.

Scheduled maintenance activities including applying security patches and carrying out data and system backups will be scheduled to take place outside the supported hours of operation

In some emergency situations it may be necessary to carry out maintenance activities within the supported hours of operation, with the result that the Salesforce Support Service is unavailable. Any such emergency changes will be agreed with Post Office.

The Salesforce Support Service will not normally be available outside of the hours stated in section 2.3.1 except when scheduled or emergency maintenance activities are taking place.

Monitoring of the platforms, database, and application for the PerspecSYS data residency solution:

a.Automated monitoring and raising of incidents related to hardware, operating systems, database management systems, network components, scheduled activities, and alerts raised by the PerspecSYS application

b.24x7 monitoring by SMC for automatically raised incidents.

The impact of loss of datacenter have written in SVMSDMPLA0002- HNGX services business continuity plan, in section 11.2 , Item number 238 to 240.

6.4 Network Services

6.4.1 Network Capacity into Data Centres

The capacity of the access network to the data-centres in IRE11 and IRE19 has been designed to ensure that each data-centre is capable of fully supporting the predicted maximum network traffic.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6.4.2 Data Centre Network Topology

The Data Centre network is based on four core Cisco 6513 switches (two per site) and four Access 6513 switches with resilient ASA5540 based firewalls between the Core and Access layers. Each core switch has a firewall module and an ACE (Application Control Engine) module. Both the ACE and the FWSM have redundant connections as well as the main MSFC interconnect. The FWSMs interconnect using a heartbeat (not ISL) over a Dot1Q 20G link, and the FWSMs interconnect over a 4GB link carrying a heartbeat. It is possible for any (or more than one) of the modules to fail and have traffic routed between switches to different modules in different chassis'.

All network components are deployed in pairs at each Data Centre. The only exception is the Vodafone link which has a single CE router and single HO router.

Every discrete server that connects to the network has at least two NICs. Each NIC connects to a different network switch. The NICs are configured in an Active/Passive configuration (not load balanced) with Switch 1 as the preferred switch.

More information is available in:

Architecture (ARC/NET/ARC/0001)

Data Centre LAN Design (DES/NET/HLD/0004)

Wide Area Network Design (DES/NET/HLD/0009)

Branch Access HLD (DES/NET/HLD/0014)

Transit LAN Design (DES/NET/HLD/0015)

Figure 31 below gives a very high level view of the switch connectivity that forms the basis of providing a resilient Data Centre network service with DR capability. The inter-site links are leased dark fibre from Virgin (NTL) with an FTEL service. The links do not share any single point of failure, and there is a minimum 10m component separation at all points along the route.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

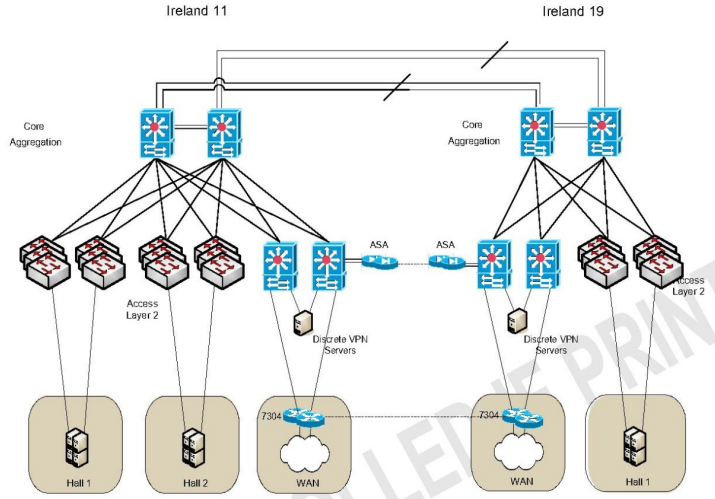


Figure 31

Connections from outside the Data Centre are via dedicated Vodafone 155 mbps circuits, one to each Data Centre. Resilience of client connections is provided via the inter-site link.

The segregation is such that a DR Business Continuity Test should only need to consider failover of the core switch layer. The Access layer is covered by normal component resilience testing.

6.4.3 Data Centre Disaster Recovery (DR) - Network

The two data centres normally operate in an active/DR manner, with IRE11 as the normally active site. IRE19 will be used as a test facility under non-DR conditions. Although applications and services from the data centres generally operate as active/DR, the network operates active/active at all times (including the Utimaco VPN servers). However, since a data centre failover requires the BAL servers to retain the same server IP addresses, along with the same VIPs advertised towards the clients, these elements of the network operate in an active/DR configuration to prevent problems associated with the advertisement of duplicate subnets.

Under normal circumstances Live traffic on the clear (unencrypted) side of the VPN servers will be steered towards IRE11 using an intercampus VLAN. Traffic will not be load balanced across parallel paths. Test traffic will be steered towards IRE19 in a similar manner. Support staff will have connectivity to either site.

Failure of data centre WAN equipment on the preferred path (local CE and/or local Handoff router) results in traffic re-routing via the equivalent router in IRE19 and the intercampus LAN.

Invocation of DR, where the operational data centre is transferred from IRE11 to IRE19, is a manual process that takes up to two hours. Network failover to DR uses scripting, where necessary, to manage the changeover, which facilitates the reconfiguring of the server estate with the same IP addressing as used in IRE11.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

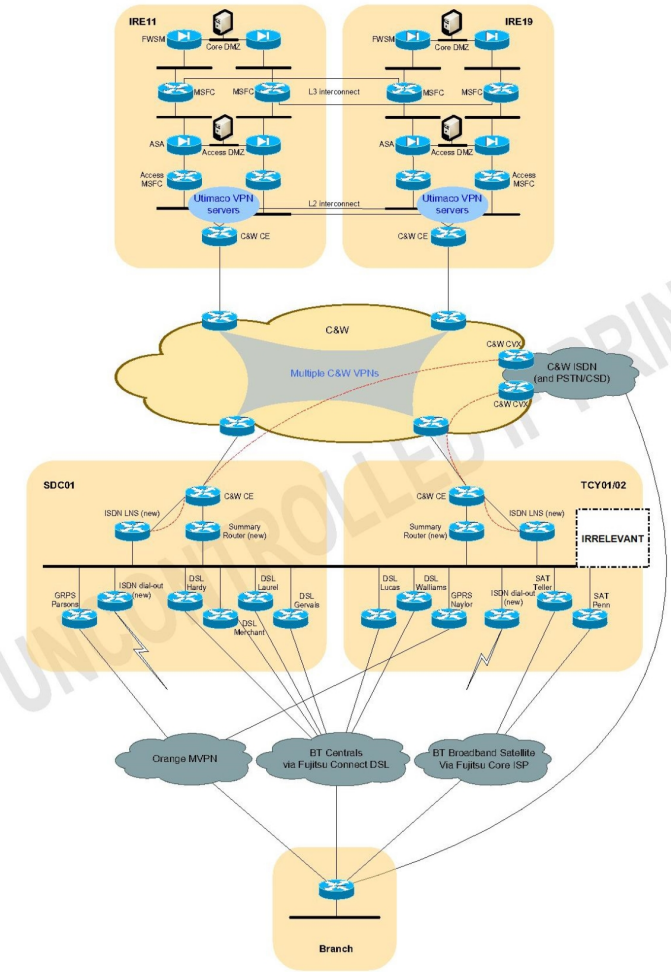


Figure 312

Branch access network end-to-end

6.4.4 Fujitsu Network Management Systems (NMS / NNM)

NMS platform resilience is achieved by the deployment of two management platforms, one in each data centre. Should a single platform fail, the equivalent platform at the other data centre will continue

© Copyright Fujitsu Services Limited 2014

FUJ00232658

operations, however the normal mode of operation is active / active. This mode of operation is important as it is essential that when DR is invoked the network fail-over activities can be performed without having to wait for network management system platform provisioning to take place.

Reference: Network Management System HLD (DES/NET/HLD/0012).

6.4.5 Vodafone Network Management Centre

The Vodafone Network Management Centre is a 24-hour manned facility based at Bracknell. In the event of the unavailability of the Bracknell site the Vodafone NMC shall relocated to the Watford disaster recovery site.

6.4.6 Vodafone ISDN Availability

The Vodafone ISDN LNS platforms (one in each data centre) are located in SDC01 and TCY02.

BT's 21CN network architecture means that both ADSL and ISDN circuits may share the same aggregation or metro-area network from the BT exchange.

For all outlets there are single points of failure within the BT network, namely at some local serving exchanges where an ISDN2 line to a PO outlet terminates, however overall Branch availability is increased through the use of Branch Router secondary connection type (e.g. WWAN) which activates in the event of any availability problems within the ISDN network.

UNCONTROLLED IF PRINTED

6.4.7 Fujitsu Services SDC01 & TCY01/02 Data Centres & ADSL Service

The Fujitsu Services ADSL IPStream infrastructure utilises four Points Of Presences in the Fujitsu Services Southern Data Centre 01 comms rooms 1 and comms room 2, and two more at TeleCity01 and TeleCity02 Data-centres. The DLS LNS routers are configured to provide contingency across the six Points Of Presence.

BT's 21CN network architecture means that both ADSL and ISDN circuits may share the same aggregation or metro-area network from the BT exchange.

Asymmetric Digital Subscriber Line (ADSL) technology has been implemented within the Vodafone MPLS data network. ADSL served Post Office Outlets have a connection through a specific Vodafone Broadband Access Servers and therefore for ADSL outlets this is a single point of failure within the Vodafone MPLS network.

This would result in the loss of communication with a number of PO outlets, but 'local exchange failures, would be limited to a small geographical area, however overall Branch availability is increased through the use of Branch Router secondary connection type (e.g. WWAN) which activates in the event of any availability problems within the ADSL network.

6.4.8 Wireless WAN Availability

Although the Wireless WAN (WWAN) network will mainly be used as a secondary network connection type, there will be some cases where it will be used as the primary network connection type, such as with mobile vans.

The Orange and Vodafone networks have a high level availability within the core of the networks; however it is a non-guaranteed & contended service at the wireless access point,

In the situation of the WWAN being the primary network connection type then branch network availability will be directly subject to the network provider's availability.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6.4.8.1 Orange Wireless WAN - Availability & Resilience

The Orange MPLS service and hand-off is designed for high availability and resilience by providing N+1 at various elements in the end to end service. There are two geographically diverse Orange GGSN nodes, Orange resilient MPLS network, dual leased circuits for different Orange points of presence with corresponding CE routers delivered to two Fujitsu data centres. On from this there are dual WWAN LNS routers capable of terminating 8000 PPP sessions, one per data centre.

6.4.8.2 Branch Router Availability

The MTBF (uptime) of the Sarian DR6410 router along with a reduced MTTR (downtime), combine to improve overall availability.

6.4.9 Transaction Network Services UK LTD (TNS)

The network links provided by Transaction Network Services are currently limited to one X25 link from IRE11 and one from IRE19 to HSBC Merchant Services (HMS) for the DCS online debit card transactions. Data can be transferred by either route.

6.4.10 Post Office Limited Northern Data Centres

Access to the POL NDC site is via Vodafone separately routed Vodafone IP Select network connections. The resilience of these circuits is also high due to the fact that there is no common point of failure between each site and the data-centres. Each data-centre has two separately routed Vodafone IP Select network connections back to two separate Vodafone Synchronous Network Access Points (SNAPs). Connectivity between SNAPs and the POA data-centres is provided by Vodafone fibre, via the Vodafone backbone.

UNCONTROLLED IF PRINTED

6.5 The Security Service

6.5.1 Key Management Servers and Database – HNG-X

Resilience of the system is obtained by deployment of 2 Key Servers in IRE11 (the primary data centre).

Resilience of the Key Server service is managed through the Key Server Client that applications use to interface to the Key Server. .

6.5.2 KMNG Workstations

KMNG workstations are based in BRA01, exist in a secure room, on a dedicated business network, fire-walled and separate from the Fujitsu corporate network, and are operated by the HNG-X Security Team.

The KMNG workstations are replicated at the designated disaster recovery site (LEW02), and (after initialisation) can be used in the same way as the normal live version to facilitate POA business operations. Bug-fixes, design or configuration change to the application or platform is replicated at the disaster recovery site as soon after issue as possible.

6.5.3 Tivoli Infrastructure

© Copyright Fujitsu Services Limited 2014

FUJ00232658

With the exception of the Certification Authority Workstation (which is not connected to the network), all processes in the Key Management Centre are monitored by Tivoli, which will raise appropriate alarms if a process stops running.

6.6 Branch and Estate Change Management Recovery and Resilience

The Estate Management Infrastructure will be available to service requests on a 24 hour basis. Where there is a requirement to update any of the component platforms comprising the service there will be limited periods of un-availability out of normal business hours (08:00 - 18:00) while this takes place. The Radius servers will provide an uninterrupted service during this period.

6.6.1 Estate Management Database Server (EST)

In general terms the EST clients, with the exception of the Radius Servers and the Boot Platform, will not require data in an interactive mode out of normal working hours, and will tolerate EST non-availability, except at those times where scheduled activities to retrieve data from EST occur. The Boot Platform is used during branch equipment replacement and installation activities which includes the Branch Router Rollout programme. The resilience model for Release 1 of HNG-X is the provision of good Radius resilience and conventional recovery profiles for all other systems that would limit downtime to a period commensurate with the re-instancing of a blade in the case of a physical hardware failure and recovery from database image where database corruption has occurred. The time lost in this instance should be limited to no more than 2 hours.

The EMDB Server will be an SQL Server 2005 and Tomcat based platform with the following characteristics:

- High availability for read operations.
- Low number of write operations.

Database backups will be scheduled every evening to facilitate point in time recovery in the event of database corruption, operational failure, or hardware failure, and will facilitate point in time recovery using the transaction logs which will also be SAN based. The operational filestore will be maintained on SAN to facilitate recovery in the event of Site failure.

6.6.2 Boot Platform

The Boot platform is responsible for ensuring that the installation of counters and Branch Routers is uninterrupted especially during periods of high activity such as Branch Router rollout. There are two operational Boot Platforms, these will be addressed in turn (no attempt to load balance) by Branch Router and Counter platforms, if an attempt to contact the primary fails then the secondary will be selected.

6.6.3 Branch Change Management Server (BCMS)

BCMS Resilience is not critical for the operation of the HNG-X Service, therefore a period of up to 24 hours is manageable in the event of failure.

The primary server is in BRA01, with a DR Instance located at the POA DR Site (LEW02) to be used in the event of a primary site failure.

6.6.4 Radius Authentication

CHAP authentication requires that the EMDB maintains an operational profile that will service the Radius servers for connection requests during normal working hours. Resilience will be provided by the client

UNCONTROLLED COPY

FUJ00232658

application on the Radius platform maintaining a cache of all CHAP secrets on all Radius platforms that are periodically refreshed to provide up to date information.

6.6.5 Hardware Resilience for Estate Management Platforms

The EMDB and the Boot Platform are provisioned as individual vBlades within a Blade Frame Server. The Blade Frame technology effectively gives each server platform a fully resilient virtual LAN connection to their respective Network Security Domains in the Campus Network.

The Blade's storage is supplied via a common SAN that is configured with distinct areas for Operating Systems and Paging, Binaries and Data.

In the event of a single platform Blade or vBlade failure, there are four likely failover scenarios.

- Re-provision the failing platform on a spare (v)Blade in the Blade Frame.
- Re-provision the failing platform on a spare (v)Blade in another Blade Frame.
- Restore Image on new (v)Blade in the Blade Frame
- Restore Image on new (v)Blade in another Blade Frame

In both of the re-provision cases above, the entire platform's storage is immediately accessible via the SAN.

SAN replication ensures that there is a current copy of the Database Storage media including transaction and rollback logs present and available at the DR Site in the event of a Site Failover.

6.6.6 EMDB Database Backups

EMDB uses a hot backup every night with no loss of service.

6.7 Reconciliation Service

This runs on the Main Host Server

6.7.1 Main Host / Data Warehouse

This provides the capability to monitor and report on virtually every hardware component and software application comprising the Horizon solution in general and the Data Warehouse/MIS solution in particular.

It also allows a significant amount of automation to be introduced into the overall HNG-X capability, which in most situations allows more timely resolution of any failures that are experienced.

The Data Warehouse runs, on the HNG-X Main Host server, a Fujitsu-Siemens Primepower platform under Solaris.

Commented [AP3]: Check if it is now on blade frame

The server is provided with dual power supplies and uses the EMC Symmetrix DMX3 which is a fully resilient enterprise class storage array spanning both Data Centres, and has no internal single points of failure.

Resilient components include:

- Disks (EMC Raid)
- Power
- Memory
- Internal Processors

6.7.2 Main Host Server Resilience

UNCONTROLLED IF PRINTED

FUJ00232658

There is a second Main Host server in the same Data Centre in IRE11 which can be used in the event of a total unrecoverable failure on the primary server. As a guide it takes approximately two hours to fail-over.

6.8 POLSAP Development and Test QA Services – IRE19

The POLSAP service is treated as two separate systems, being Production and Development / Test / QA , however from the point of view of service delivery it is treated as active/active since both are used by external customers.

It is possible for the POLSAP Production service to be failed over to IRE19 without any impact on the rest of IRE11 which provides the HNG-X service to outlets (the POLSAP non-live services that were running in IRE19 are not available during a Production fail over). Network load balancing uses ACE in HNG-X and advertises a VIP to the external customer for the POLSAP service which allows them to easily access the POLSAP live service from either data centre.

The Development, Test and QA systems which run in IRE19 have no failover facility.

6.9 System Management Service

6.9.1 System Management Platforms – Resilience

All of the platforms run using blade technology and use the spare blade capability in the event of a server failure. The EMD and EES have additional resilience via a secondary server in IRE11. The EFS servers operate in pairs giving dual access to services.

All data is replicated to IRE19 to facilitate a data centre failover.

Platform Name		How many	CPUs	Software Item	Criticality
EMM	System Enterprise Monitoring Server	1	2	TEMS	
EUI	System Enterprise User Interface Server	1	2	TEPS	H
EMD	System Enterprise Monitoring Display	2	2	Object Server	
EES	System Enterprise Event Server	2	2	Object Server	
EAS	System Availability Server	1	4	RAD	
EFS	System Enterprise Fan-out Server	40	2	Proxy Probe	
EDS	System Enterprise Database Server	1	4	Database Repository	H

6.9.2 Loss of Network Communications to IND49/STE04

In the event of IND49 becoming isolated, due to the loss of network devices, SMC off-shore staff could relocate to Pune (IND 46) which has a separate internet connections to TCY01 and TCY02 in the UK. Up to twelve hours has been allowed for this from the time a decision is taken. During the relocation process SMC staff could request assistance from MSS or SSC.

6.9.3 Buildings – Blackpool BLA01 – MSS North/ SMG

Commented [AP4]: Needs updating

With the loss of BLA01 it is planned that staff would relocate to WAR07 or work from home.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6.9.4 Buildings – IND49 - SMC

With the loss of IND49 it is planned that the off-shore SMC staff would relocate to Pune. Up to twelve hours has been allowed for this from the time a decision is taken.

6.9.5 People - MSS

The MSS is operated on a 'two shift' basis. In the event of the loss of employees from one shift, staff from the unaffected shift would be available.

6.9.6 People – SMC in IND49

The SMC is operated on a "24 by 7" basis. In the event of the loss of employees from one shift in IND49, staff from the unaffected shift teams would be available to transfer to an alternative site, or operate from Pune.

6.10 Operational Support Services

6.10.1 The Systems Operate Service

6.10.1.1 Activation

Once an event has occurred that will impact the provision of the UNIX and NT Service and/or the Operational Service, then in all instances the 'Activation' procedure will be invoked and a TRIOLE for Service incident will be raised with the SMC or MAC.

6.10.1.2 Loss of Documentation server

The document server is part of the office infrastructure and is located in the IRE11 operation-centre. A secondary document server is based in IRE19. The contents of the secondary server are automatically updated at 19.00 each evening from the primary server. The secondary documentation server is accessed as part of the Systems Operate Services Business Continuity Test to confirm its functionality and accuracy.

Commented [AP5]: Which Documentation server? Ask Adrienne

6.10.1.3 Loss of Electrical Power

In the event of a power failure the UPS will activate and keep all FS systems up and running whilst the standby generator activates. The backup generator will take effect approximately 30 seconds after the failure. The lighting and air conditioning will have no power [due to being non-UPS supported] for the 30 seconds it will take for the generator to start providing power. Emergency lighting will immediately be activated as the mains supply is lost.

6.10.1.4 Loss of Telephone exchange

In the event of the loss of 'land-line' telephone networks in either IRE11 or IRE19 operation-centres mobile phones would be used as a backup contingency measure. All Belfast based SOS staff are provided with company mobile phones. The Services Manager would liaise with the Major Accounts Controllers to ensure a full awareness of the situation.

6.10.1.5 Loss of the IRE11 Office area

In the event of a disaster that left IRE11 inaccessible, Support Service fail-over would be instigated in accordance with the FSCS Support Contingency site fail-over procedure. Actions to restore all the required support functions will be managed through incident management procedures as detailed in this document.

UNCONTROLLED IF PRINTED

FUJ00232658

6.10.2 Support Services

6.10.2.1 The System Management Centre (SMC)

In the event of a major incident or disaster at IND49 it is planned that the off-shore SMC staff could relocate to Pune IND46. Up to twelve hours has been allowed for this from the time a decision is taken.

6.10.2.2 POA Customer Services - Overview

Fujitsu Services POA has developed plans to provide CS operational and support services from LEW02 in the event of a disaster or unexpected incident at Fujitsu Services (POA) Bracknell. SVM/SDM/PLA/0034 (POA Crisis Management And BRA01 Disaster Recovery Plan) details the disaster recovery equipment for CS operational use at LEW02. This equipment consists of a mixture of hot and warm 'standby' equipment. The hot standby servers and workstations are connected to the live infrastructure and maintained, by the FSCS SOS at a fully operational state. The warm standby workstations are stored in a 'ready-for-use-state'.

Internal business walkthroughs are conducted on an annual basis to assess the preparedness of any new service element for implementation.

6.10.2.2.1 Incident Management

In the event of an incident occurring at Bracknell the Fujitsu Services (POA) Incident Controller for Bracknell will be informed, See SVM/SDM/PLA/0034. The Incident Controller referring to the Incident Management Plan will inform all CS Business Recovery Team Leaders of the event, instigate the raising of a TRIOLE For Service call to escalate the incident and, if necessary, contact the Fujitsu Services (POA) Crisis Management Team.

The Incident Controller will decide which CS teams and individuals are to be relocated to Fujitsu Services LEW02, other Fujitsu Services sites, or are to work form home. The Incident Management Team members will instruct the Business Recovery Team managers of the invocation of relocation and the Business Recovery Team managers shall decide which team members will be relocated.

The call will meet the MAC (Major Account Controllers) escalation criteria, so it is escalated to the Fujitsu Services (POA) Duty Manager. The Duty Manager uses the processes described in SVM/SDM/PRO/0028.

If the criteria for a Major Business Continuity Incident (MBCI) are satisfied (SVM/SDM/PRO/0028) the Duty Manager escalates the incident to the Fujitsu Services (POA) Business Continuity Manager as a Business Continuity event.

6.10.2.2.2 Peak Support Incident Management

The Peak Support Incident Management service is provided by the SSC.

The primary Peak server (peak2) is installed in BRA01 and the secondary Peak server (peak3) resides in LEW02. The database on this server is synchronised every 15 minutes over the Fujitsu Services corporate network. In addition nightly back-ups are also taken of the Peak servers and placed on to the PEAK server in LEW02.

The Peak Client is installed on the Office PCs in both BRA01 and LEW02.

Commented [AP6]: Confirm with John Simpkins if a PEAK client is used/ necessary. Surely a statement around access is via corporate LAN would suffice?

6.10.2.3 Configuration Management – Signing Server

The POA Programmes secondary Configuration Management Signing server resides in LEW02. The database on this sever is synchronised on an hourly basis with the BRA01 Signing server via the Fujitsu Services corporate network In addition daily back-ups are also taken of the Signing servers.

In the event of a disaster at BRA01 the Programme team can access the CM Signing server at LEW02 using disaster recovery laptops at least one of which is held off site.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

6.10.2.3.1 Change Control

The primary PVCS server resides in BRA01 and a secondary server resides in LEW02. The BRA01 PVCS server is replicated overnight to LEW02 PVCS server. In addition to this daily tape backups are taken off site.

To access PVCS users require either 'PVCS Terminal' or PVCS Dimensions PC Client. PC client is installed on the Office PCs in both BRA01 and LEW02.

HNG-X Dimensions is accessible to authorised users via the Fujitsu LAN. Access is either via the web interface, or via the Dimensions Serena Client.

6.10.2.3.2 Development Operational Support Live System Team (LST)

The Live System Test (LST) team, which resides within the POA Development organisation, test software changes about to be released into the live estate. This is achieved by proving the software changes on discrete test configurations that replicate the live software environment.

The prerequisites to provide this service are:

- Availability of hardware test rigs upon which the live software set can be loaded and run;
- Access to Fujitsu Services (POA) infrastructure services i.e. Peak, TRIOLE For Service, PVCS.

Disaster Recovery facilities are available at LEW02 for the LST service. This is only true for those elements of the service based in BRA01. In the even of a loss of IRE19 there would be no LST Service. There would also be no SV&I service, no POLSAP DEV or QA service, and no Credence/MDM OAT service

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

7 Preparedness Measures

Preparedness in the HNG-X context is defined as, those measures taken to ensure the technical solution and business processes supporting that solution deliver the service that they are designed to deliver, in such a way as to meet and exceed the service level.

7.1 Testing

From a technical standing, functionality is proven by testing the solution at a unit, system and business integration level.

This functional testing has been complemented by performance and security testing to ensure that the solution is both scalable and secure.

Internal business walkthroughs are conducted on a regular basis to assess the preparedness of any new service element for implementation.

In preparation for any HNG-X Release, in conjunction with Post Office Limited, a full end to end processing rehearsal and test is performed where the whole solution and supporting processes are run as if live for a period of several days.

It is usual for this to include a rebuild of all operational platforms used in the delivery of the service which further validates the accuracy of operational procedures and configuration management processes.

7.2 Service Management & Delivery

From a business perspective, this process starts by establishing very exacting and specific service level agreements with all suppliers to the HNG-X Service which are constantly monitored and reviewed.

The provision of Operational documentation for all aspects of service delivery is mandated and allows POA to ensure that the service is being delivered in a consistent way that satisfies service level requirements.

7.3 Risk Analysis

Impact & Risk Assessment contains a risk analysis of the end to end supporting services incorporated in this plan.

This identifies potential risks to those supporting services, the assessed probability of that risk occurring, the impact of that risk becoming a reality and the contingency activity or plans necessary to contain such an occurrence with minimum impact to those supporting services.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

8 Contingency Measures

Contingency measures are defined as the actions to be performed in the event of a service break to enable business impact to be minimised during the service outage prior to recovery being completed.

Contingency measures will include the recognition, activation, incident management and initiation of recovery procedures.

8.1 Recognition

The HNG-X solution includes a Systems management capability to monitor and report on events that occur upon all the platforms involved in the service delivery and counters.

The process of monitoring and managing the Network components and Routers is performed by a combination of the products HP OpenView and CISCO works.

ITM (Tivoli) is used to manage and monitor the Sun Solaris Servers and Windows platforms and to consolidate and present the status information.

The SMC monitor all services and escalate incidents to the POA Duty Manager, and depending on the severity of the abnormal circumstances that have been identified, also to the POA Business Continuity Manager.

UNCONTROLLED IF PRINTED

8.2 Activation

Once an event has occurred that will impact the provision of the NBS Service (Network Banking), then in all instances an incident will be raised with the MAC (Major Account Controllers).

There are a number of scenarios where the capability of the Systems Management environment will trigger an operational script to run upon the platform/application that has suffered the problem, to correct the failure. Operations personnel may override this.

8.3 Incident Management

Personnel at the SMC will normally perform this function. If the incident cannot be resolved by the SMC at the time of the call it will be routed to the appropriate support unit for resolution. At the same time if the incident meets the SMC escalation criteria, it will be escalated to the Fujitsu Services POA Duty Manager.

If the criteria for Cross-Domain Business Continuity Management are satisfied the Duty Manager will escalate the problem to the POA Business Continuity Manager who will own the problem as a Business Continuity event.

Note: Post Office Limited may also escalate Business Continuity events directly to the POA Duty Manager.

8.4 Initiation of Recovery Procedures

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Where this is a POA only incident, this would usually be instigated by the support team charged with supporting the equipment upon which the failure has occurred, as soon as possible, and certainly with intent to resolve the incident within the relevant Service Level Agreement.

Depending on the severity of the incident, there may be some dialogue between the Duty Manager and the support function to agree on the most appropriate course of action.

Wherever there is a Cross Domain incident, the resolution would be instigated at the time when all parties affected had agreed the course of action:

In the case of a Business Continuity incident, this would be after the Business Continuity Team had agreed a plan of action, see Section 12, Plan Activation.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

9 Recovery Of Normal Service

All aspects of the Services infrastructure within POA are managed operationally by the Core Services division of Fujitsu Services (FSCS).

As such, the process of recovering from an event causing an impact to the service will by definition involve FSCS in performing an operational activity to resume the full service.

FSCS have developed an Operations Procedures are underlying on web pages that make up UNIX & NT operational documentation from which operational and recovery processes and procedures are identified, for all possible failures in the end to end HNG-X Services.

Thus in its simplest form, normal service could be resumed by the Duty or Problem manager liaising with the support team, agreeing when the recovery action should be run, and then carrying that activity out.

Where the recovery action is dependent upon a third party, e.g. Prism or Post Office Limited, the support dialogue would take place between the support teams, and the problem management dialogue would take place between the appropriate management.

9.1 Recovery Time Objectives and Recovery Point Objectives

9.1.1 HNG-X Infrastructure RTO and RTP Objectives

The following table provides the maximum recovery time objective and the recovery point objective for the infrastructure supporting the HNG-X services.

	Maximum Recovery Time Objective	Maximum Recovery Point Objective
Storage Systems		
Audit Centera Array	Next day	Normal Service Provision
Audit Server	2 hours	Normal Service Provision
Backup Servers	2 hours	Normal Service Provision
ECC Server (or equivalent)	Next day	Normal Service Provision
Main Backup System (Disk or Tape)	2 hours	Normal Service Provision
Support Systems		
Secondary Authentication Service	15 minutes	Normal Service Provision
Antivirus Server	Next day	Normal Service Provision
Application Monitoring Server	15 minutes	Normal Service Provision
Certification Server	15 minutes	Normal Service Provision
DNS Server	15 minutes	Normal Service Provision
Domain Controllers	15 minutes	Normal Service Provision
NBX Network Observer Server	Next day	Normal Service Provision
NBX Network Probe Server	Next day	Normal Service Provision

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Maximum Recovery Time Objective	Maximum Recovery Point Objective
Network CISCO Works Server	15 minutes	Normal Service Provision
Provisioning Server	Next day	Normal Service Provision
Radius Servers	2 minutes	Normal Service Provision
Accounting Radius Servers	2 hours	Normal Service Provision
SSN Server	15 minutes	Normal Service Provision
Signing Server	2 hours	Normal Service Provision
SQL Server (ACDB, OCMS, Athene, MTAS)	2 hours	Normal Service Provision
SSC Branch Database	2 hours	Normal Service Provision
SYSMAN Enterprise Managing Server	2 hours	Normal Service Provision
SYSMAN Enterprise Monitoring Server	2 hours	Normal Service Provision
SYSMAN Enterprise Event Servers	2 hours	Normal Service Provision
SYSMAN Availability Server	2 hours	Normal Service Provision
SYSMAN Enterprise User Interface Server	2 hours	Normal Service Provision
SYSMAN Enterprise Database Server	2 hours	Normal Service Provision
SYSMAN Enterprise Provisioning Server	2 hours	Normal Service Provision
SYSMAN Enterprise Fanout Server	2 hours	Normal Service Provision
SYSMAN Enterprise Staging Servers	2 hours	Normal Service Provision
SYSMAN Enterprise Legacy manager	2 hours	Normal Service Provision
SYSMAN Enterprise Monitoring Display	2 hours	Normal Service Provision
Network switches	24 hours	Normal Service Provision
Network routers	24 hours	Normal Service Provision
Cable failures / mis-cabling	24 hours	Normal Service Provision
Data Exchange Server		No data to recover
Key Management Server		Normal Service Provision
Main Host (Batch Database Server)		Normal Service Provision
		Normal Service Provision
		Normal Service Provision
		Normal Service Provision
		Normal Service Provision

UNCONTROLLED IF PRINTED

9.1.2 HNG-X Services Disaster Recovery RTO and RPO Objectives

The following table provides the maximum recovery time objective (RTO) and the recovery point objective (RPO) for the HNG-X services following a major incident or disaster that causes POA to invoke a fail-over to IRE19.

FUJ00232658

Service Description	Maximum Recovery Time Objective	Maximum Recovery Point Objective
Core Solution and Network Banking, including: Branch Database Servers Client File Transfer (DCS, ETU, Banking) DCS Servers FTMS TIP Local & Track and Trace NBX Banking Agents Branch Access Layer servers NPS Servers (Database)	2 hours	Normal Service Provision
All remaining Services excluding POL-FS: ETU & DVLA online Servers PAF & APOP Agent Servers TES Application Servers APOP Servers (Database) (Priority would be given to any services crucial at time of DR e.g. DVLA if at end/beginning of month. PAF if at Christmas mailing peak period)	5 hours	Normal Service Provision
Security Management Service	Not defined	
Branch Change Management Service	Next working day	Normal Service Provision
Estate Management Service	Not defined	
Network Services	2 hours	Normal Service Provision
Data Centre Operations Service	2 hours	Normal Service Provision
SAP Development and QA-Test Systems	Not defined	
System Management Service	2 hours	Normal Service Provision
Support Services	2 hours	Normal Service Provision
System Operate Services	2 hours	Normal Service Provision
Reference Data Management Service	Next working day	Normal Service Provision
Reconciliation Service	Next working day	Normal Service Provision
Service Integration Service	Not defined	
Receipt Template Service	Not defined	
Service Management Service	Not defined	
Message Broadcast Service	Not defined	
MIS Service	Next working day	Normal Service Provision
Third Line Support	3 hours	Normal Service Provision

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Fourth Line Support	Not defined	
Branch Network Service	Not defined	
Third Party Management Service	Not defined	
Service Desk Service	3 hours	Normal Service Provision
POL-FS (Reduced Performance Provision)	48 hours	Normal Service Provision

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

10 Impact & Risk Assessment

10.1 Risks Identified Against the HNG-X Support Services

The matrix below details the identified risks to the data processing elements of the HNG-X Services.

The nature of the service changes between the day and night schedules, however to improve the usability of this plan the worst case Critical Impact Timing for each service element incident has been used.

Day time processes are primarily concerned with Counter transactions and Help Desk processes, Night time processes are primarily concerned with preparing for the next counter day, and processing the transactions that have been processed during the Post Office Core day. This is reflected in the actions against the identified risks.

As a matter of normal operational practice, a call would be placed against MAC Team if any of the identified risks materialised.

The intention is that the list of identified risks (Section 10.2) can act as a guide to personnel assessing and managing any incident affecting the HNG-X service.

The matrix contain a column identified as probability with a range of 0 to 4. These estimate the probable risk of failure. It must be emphasised that these are not percentages and should be considered simple weighting factors.

UNCONTROLLED IF PRINTED

As a guideline the following occurrence ratings have been allocated:

Rating	
0	Less than one incident is predicted per year
1	One incident is predicted per year
2	Two incidents are predicted per year
3	Approximately three incidents are predicted per year
4	Ensure that appropriate contingency measures are taken e.g. duplicate routing or the holding of spares on site.

The probability of failure of major elements of the service is low because:

1. There has been a high level of resilience and duplication built into the infrastructure.
2. Extensive validation has been performed upon the infrastructure.
3. The Fujitsu Services POA project team has developed a vast knowledge of component failure and service availability over the past three years.

Where a Potential MBCI or MBCI (Major Business Continuity Incident) has been designated as being triggered and there is no reference to section 11.3 then there are no further contingency actions to be performed over and above normal operational incident processes and the actions already identified within the risk table.

If a failure occurs during or after any hardware or software change, then consider regressing the change.

Please Note: This business continuity plan is one of four. If the POA Duty Manager (or other authorised person) is unable to find the failed infrastructure components in this plan they are mandated to refer to:

- HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002);

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- HNG-X Support Services Business Continuity Plan (SVM/SDM/PLA/0001);
- HNG-X Engineering Business Continuity Plan (SVM/SDM/PLA/0030)
- HNG-X Security Business Continuity Plan (SVM/SDM/PLA/0031)

The risk assessment identifies the Critical Time Factors for activation of contingency measures as defined in the Business Continuity Framework SVM/SDM/SIP/0001. For on-line service, e.g. NBX and DCS the CTF is identified against Post Office Core Day Processing, whilst for file transfers, e.g. APS and TPS the CTF is identified against Post Office Non-Core Day Processing.

The 'Impact' column contains a statement indicating the level of business disruption. This impact from a Support Service Perspective refers to a potential impact to primary services, e.g. APS, TPS, as well as software drops, Reference Data releases, counter management etc.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

10.2 Trigger Tables for HNG-X Support Services

Notes:

1. The following trigger table details the non-availability of the Primary component, and the Primary and Standby components.
2. The non-availability of support services Standby servers and some network components should be treated as a loss of resilience and resolved via normal incident management processes.
3. Branch Network Resilience - No entries have been included in this table for the loss of ADSL and the ISDN/GSM service for outlets where BNR has been implemented. If there is a loss of online services for Branches that have lost their primary connection through ADSL and secondary through ISDN/GSM please treat the failure as an MBCI Trigger and the POA BCM is to inform the POL BCT.
4. No entries have been included in this table for the POLSAP Development or QATest infrastructure as there are no contingency or DR requirements for these services. Refer to SVM/SDM/OLA/0872 for details of the OLA for these services.
5. There are two possible failure scenarios for any virtual server using a Blade. There could be a failure of some kind with ONLY one specific virtual server, leaving the other virtual servers on the same Blade unaffected, or there could be failure of the whole Blade causing up to 5 separate virtual servers to fail at the same time.
6. In the trigger table below all service that are provided from a Bladeframe virtual server should initially restart on one of the spare physical Blades (assuming that it has been configured for an auto restart), therefore the entries in this table assume this initial capability.
    - normally a failed physical Blade will be identified by at least two alerts:
    - there should be an alert for each lost virtual server that was running on the failed physical Blade (up to 5 virtual servers)
    - there should be an alert for the hardware failure of the specific physical Blade
    - the lost virtual servers should be restarted automatically (unless specifically set to NON-auto start)
    - the SMC and support teams:
        - will verify that functionality has restarted for all lost virtual servers
        - will resolve the problem with the failed physical Blade

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

- bring the failed or replaced physical Blade back into service at an agreed time
- confirm normal operation and return the spare physical Blade back to being the spare

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Note the following parts of the HNG-X Solution are covered in SVM/SDM/PLA/0002 HNG-X Services Business Continuity Plan

POL NDC to Data-Centres
Data Centre Local Area Network (Client and Server Access)
POL SAP
Data-centres Buildings
Data-centres/Clients TIP and AP Gateways
Data Centres Database (Host) Server/EMC Disc Array,
Network Banking Infrastructure and T&T Harvesting Agent and Transaction Journal.
Debit Card Infrastructure (Note: ETS also utilises some DCS infrastructure)
ETS Specific Infrastructure
DVLA, PAF, APOP,GWS,CWS and MoneyGram Web Services
Data-Centre LANs and Supporting WANs
Data-centre – Branch Access Layer and Branch Database
Data-centre LAN Infrastructure (to Branches)
Network Links to Branches
Post Office Branches
Reference Data Service - Specific Infrastructure

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Index to trigger tables

Security Management Service	1
Main Host / Data Warehouse / Disk Arrays	16
Branch & Estate Management	21
BRA01	61
IRE11/ IRE19	81
IND49/ IND46 (SMC)	112
BLA01 (MSS, SMG)	116
WAR07 (POA Networks)	118
CRE02	119
Miscellaneous	120
Vodafone	128

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
	BladeFrame Resilience - See SVM/SDM/PLA/0002					
	Security Management Service					
1.	Key Management Workstation (KSN)	Failure of BOTH Workstations in BRA01	0	4 hrs	Unable to operate Key management functions. Impact: Fujitsu Services / POL	Resolve via Incident Management Use the DR / Backup Workstation at LEW02. **Potential MBCI** **Inform POL BCT**
2.	Key Server (KMN)	Failure of the Primary Key Server (IRE11)	1	24 hrs	The alternative active instance shall provide service whilst the fail-over to the spare is completed No impact	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
3.	Key Server (KMN)	Failure of the Primary AND Secondary Key Servers (IRE11)	0	4 hrs	No Keys can be changed The service will not be available until the fail-over to a spare Blade is completed Impact on POL / Fujitsu Services	Resolve via Incident Management.
4.	Key Management Firewalls	Primary and secondary Firewall Failures	0	4 hrs	No access to Key Management service No Keys can be changed Impact on Fujitsu Services / POL	Resolve via Incident Management. **Potential MBCI** **Inform POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
5.	Intrusion Prevention Management Server (IPS)	Failure of the Primary Server (IRE11)	1	4 hrs	No loss of service since the alternative server will process the data from branches The service will operate via the alternate data centre until the fail-over to a spare Blade is completed No Impact	Resolve via Incident Management.
6.	Intrusion Prevention Management Server (IPS)	Failure of the Primary Server (IRE11) AND Secondary Server in IRE19	0	Immediate	No data from branches can be processed until the fail-over to a spare Blade is completed Impact on POL / Fujitsu Services	Resolve via Incident Management.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
7.	Hardware Security Module (HSM)	Failure of a single Module in either IRE11 or IRE19 **IRRELEVANT** **IRRELEVANT**	1	2 days	Service will be maintained by one of the other HSMs No Impact	Resolve via Incident Management
8.	Vulnerability Scanner Server (VNS)	Failure of the Server (IRE11) Note: there is no secondary server	1	4 hrs	No scanning can be performed until the FS1000 server is repaired Impact on Fujitsu Services	Resolve via Incident Management.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
9.	Audit Server (ARC)	Failure of the Server (IRE11) Note: there is no secondary server	1	4 hrs	Potential delay in capturing audit data. The service will not be available until the fail-over to a spare Blade is completed Impact on Fujitsu Services	Resolve via Incident Management
10.	Firewall Security Management Server (NFM)	Failure of the primary server in IRE11 Note: there is no secondary server	1	4 hrs	Potential delay in managing some aspects of the Firewall system. The service will not be available until the fail-over to a spare Blade is completed Impact on Fujitsu Services	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
11.	NT Domain Controllers (DOX)	Loss of a single controller - IRE11 or IRE19	1	8 hrs	Potential loss of ability of a service to connect into the required Secure Domain The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact:**	Resolve via Incident Management Connection will complete via one of the other Domain controllers (there are 6 in each data centre)
12.	Secure Access Server (SSN)	Loss of a single server in either IRE11 & IRE19	1	8 hrs	Potential loss of ability to access systems via a specific route for Support teams The service will not be available until the fail-over to a spare Blade is completed Minimal **Impact: Fujitsu Services**	Resolve via Incident Management There are 6 SSN servers running as Active / Active (3 in each data centre)

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
13.	Domain Name Server (DNP)	Loss of the primary server in IRE11	0	4 hrs	Loss of ability for services to access Domain name related information The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact:**	Resolve via Incident Management Secondary server also available (DNS)
14.	Active Directory Domain Controllers (ACD)	Loss of a single controller - IRE11	1	8 hrs	Potential loss of ability of a service to connect into the required Secure Domain The service will fail-over to a spare Blade. **No Impact:**	Resolve via Incident Management Service should continue via the second Controller in IRE11

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
15.	Network Radius Server (NRS)	Failure of a single server in either IRE11 or IRE19 There are 2 servers in each data centre	1	8 hrs	Limited potential for authentication failures. Service will be maintained by one of the other 3 servers An alternative active instance shall provide service whilst the fail-over to the spare is completed No Impact	Resolve via Incident Management
16.	Reverse Proxy Server (NRP)	Loss of a single server in either IRE11 & IRE19	1	NA	Loss of single appliance in Ire11 results in IP SLA tracked routing failover to remaining appliance in Ire11. Loss of single appliance in Ire19, under normal operation conditions has no effect. No impact	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
17.	Reverse Proxy Server (NRP)	Loss of a Dual server in either IRE11 & IRE19	0	NA	Loss of two appliances in Ire11 would result in the DR appliance being used, this would happen automatically and IP SLA route tracking would route to the DR appliance in Ire19. No impact	Resolve via Incident Management
	Main Host / Data Warehouse / Disk Arrays					
18.	IRE11 Database Server (DAT)	Primary Database (DAT) Server hardware, software or Maestro failures			See SVMSDMPLA0002 Section (E) Data Centres Database (Host) Server/EMC Disc Array	
19.	IRE11 Database Server (DAT)	Primary and Secondary Solaris Database (DAT) Server hardware, software or Maestro failures			See SVMSDMPLA0002 Section (E) Data Centres Database (Host) Server/EMC Disc Array	
20.	IRE11 / IRE19 – EMC Disc Array	For all part or total failures			See SVMSDMPLA0002 Section (E) Data Centres Database (Host) Server/EMC Disc Array	

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
21.	MIS Client	All MIS Clients at BRA01 for any reason	1	5 days	No impact. Just loss of resilience as the MI service is no longer dependent on the MIS clients	Resolve via Incident Management. If required another MIS client is available at STE04 in the machine room.
22.	Data feeds to Data Warehouse	Loss of one or more data feeds from other services for any reason	3	1 to 5 days	The Data Warehouse will wait for the feed to become available and then continue processing **Impact: , Fujitsu Services**	Resolve via Incident Management Either resolve the problem at source system or switch to Secondary system – time of day and day of week will contribute to decision. May be possible to use a dummy feed and run the real feed later.
	Branch & Estate Management					
23.	Boot Server (BPL)	Single server total failure	1	24hrs	The alternative active instance shall provide service whilst the fail-over to the spare is completed No impact	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
24.	Boot Server (BPL)	Both servers total failure	0	8 hrs	Delay in implementing outlet changes and the replacement of base & router units at branches The service will not be available until the fail-over to a spare Blade is completed Impact on POL / Fujitsu Services	Resolve via Incident Management
25.	Branch Change Management (BCMS) Workstation (BPM)	All Workstations unavailable at primary site – CRE02	0	24 hrs	Delay in entering new Outlet changes whilst some staff relocate to the alternate site. Impact POL / Fujitsu Services	Resolve via Incident Management Use workstations at the alternative Fujitsu Services site, BRA01.
26.	Branch Change Management Server (BCMS)	Failure of primary server in BRA01	1	24 hrs	Delay in entering new Outlet changes Impact POL / Fujitsu Services	Resolve via Incident Management Consider enabling the DR server in LEW02.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
27.	Estate Management Database Server (EST)	Loss of server (note: there is no secondary server)	1	4 hrs	Delays in processing Branch change data. Possible loss of Radius authentication The service will not be available until the fail-over to a spare Blade is completed **Impact: Fujitsu Services / POL**	Resolve via Incident Management
28.	Enterprise Monitoring Manager Server (EMM)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss of monitoring of systems. Loss of access to historical event data. The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
29.	Enterprise User Interface Server (EUI)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss of ability to diagnose system faults The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management
30.	Enterprise Management Server (EMS)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss of software distribution and inventory functions. The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management
31.	Enterprise Database Server (EDS)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss of the ability to provision (build) other servers. The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
32.	Event Reporting Platform (ERP)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss reporting capability The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management
33.	Enterprise Provisioning Manager (EPM)	Loss of server (Note: there is no secondary server)	1	2 hrs	Possible loss of software distribution and the ability to provision (build) other servers. The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management
34.	Enterprise Event Server (EES)	Loss of both primary and backup servers in IRE11 This is a two server configuration running as Active / Standby	0	2 hrs	Possible loss of event collection and processing. The service will not be available until the fail-over to a spare Blade is completed **Impact Fujitsu Services**	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
35.	Enterprise Monitoring Display Server (EMD)	Loss of both primary and backup servers in IRE11 This is a two server configuration running as Active / Standby	0	2 hrs	Possible loss of aggregation and display of events The service will not be available until the fail-over to a spare Blade is completed **Impact Fujitsu Services**	Resolve via Incident Management
36.	Enterprise Availability Server / Real time active Dashboard (EAS) / (RAD)	Loss of server in IRE11 (Note: there is no secondary server)	1	8 hrs	Possible loss of Business Systems View of Events to the RAD tool The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management
37.	Enterprise Management (Security) Server (EMS)	Loss of server in IRE11 (Note: there is no secondary server)	1	8 hrs	Possible loss of Security related services for SYSMAN The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact**	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
38.	Enterprise Fan-Out Server (EFS)	Loss of a single server in IRE11 (Note: there are 40 EFS servers in IRE11 configured so that there is a primary and backup capability)	1	8 hrs	Possibility that distributed Event Management clients will not be able to "login" to System management functions **Minimal Impact**	Resolve via Incident Management This is effectively a two server configuration for each client running as Active / Active
39.	Enterprise Boot Server (EBS)	Loss of a single server in IRE11 or IRE19 (There are two servers (active / active) one in IRE11, one in IRE19)	1	8 hrs	Possible loss of ability to take-on new data centre hardware Impact: Fujitsu Services	Resolve via Incident Management Service should continue via the server in the alternate data centre
40.	Corporate Data Exchange server (DXC)	Loss of both servers IRE11 & IRE19 This is a two server configuration running as Active / Active.	0	8 hrs	Loss of ability to transfer data between the secure POA systems and Fujitsu Corporate systems The service will not be available until the fail-over to a spare Blade is completed **Minor Impact: Fujitsu Services**	Resolve via Incident Management .

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
41.	Internet Data Exchange Proxy (DXI)	Loss of server in IRE11 or IRE19	1	24 hrs	None	Resolve via Incident Management Active-active resilience will continue running the required services.
42.	Internet Data Exchange Proxy (DXI)	Loss of all servers in IRE11 and IRE19	1	Immediate	Loss of ability to transfer data over the Internet to Third Party Suppliers Services affected: Kahala, Post Code Anywhere, ADSL Checker. **Impact: Fujitsu Services / POL / Suppliers**	Resolve via Incident Management
43.	SSC Support Server (SSC)	Loss of server in IRE11 (Note: there is no secondary server	1	2 hrs	Loss of ability for SSC to perform some support activities The service will not be available until the fail-over to a spare Blade is completed Minor Impact: Fujitsu Services	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
44.	SMC Web server	Loss of primary server in IND49	2	> 4 Hrs	Various information including SMC KELs would not be available **Minimal Impact: SMC, Fujitsu Services**	Resolve via Incident Management. Switch to secondary server
45.	Data-centres to SMC POA Network	Any loss of single connection	1	24 Hrs	Possible slowing of access from SMC. **Impact: SMC**	Resolve via Incident Management. Networks to diagnose and resolve. Dual connection to systems through IRE11 or IRE19.
46.	Data-centres to SMC POA Network	Any loss of both connections	0	Immediate	No system management capability, no view of the live services **Impact: SMC, Fujitsu Services, POL**	Resolve via Incident Management If total loss and not resolved within 2 hours may need to initiate contingency plan / site relocation. **Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
47.	Data-centre to IRE11 (MSS) POA Network	Any loss of connection	1	8 Hrs	Minimal impact dual connection to systems through IRE11 or IRE19 **Impact: MSS, Fujitsu Services, POL**	Resolve via Incident Management. Networks to diagnose and resolve If total loss and not resolved within 8 hours may need to initiate contingency plan **Potential MBCI** **Inform: POL BCT**
48.	Sarian Remote Management (PHU 1.5)	Loss of all 4 firewalls - IRE11 & IRE19	0	4 hrs	SMC unable to manage up to 250 PHU 1.5 systems **Impact: Fujitsu Services POL**	Resolve via Incident Management Failure of IRE11 only would require a manual failover of the Remote Manager to IRE19 **Horizon Services Potential MBCI** **Inform: POL BCT**

Commented [AP7]: Needs reviewing

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
49.	Sarian Remote Management (PHU 1.5)	Loss of both VPN Concentrators - IRE11 & IRE19	0	4 hrs	SMC unable to manage up to 250 PHU 1.5 systems **Impact: Fujitsu Services POL**	Resolve via Incident Management Failure of IRE11 only would require a manual failover of the Remote Manager to IRE19 **Horizon Services Potential MBCI** **Inform: POL BCT**
50.	Sarian Remote Management (PHU 1.5)	Loss of both Sarian Remote Management servers - IRE11 (Live) & IRE19 (DR Site)	0	4 hrs	SMC unable to manage up to 250 PHU 1.5 systems **Impact: Fujitsu Services POL**	Resolve via Incident Management Failure of IRE11 only would require a manual failover of the Remote Manager to IRE19 **Horizon Services Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
51.	Primary & Secondary Campus- Network Management LAN	Primary Radius Server	0	2hrs	**No Impact.**	Resolve via Incident Management. Switch to the secondary Radius Server.
52.	Primary & Secondary Campus- Network Management LAN	Primary and Secondary Radius Server	0	Immediate	General HNGX Services via the Vodafone Data Network **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. Reconfigure connections via secondary data-centre. **HNGX Services MBCI Trigger** **Inform: POL BCT**
53.	Performance & Capacity Database Server (SPN)	Loss of server - IRE11 No secondary server	0	8 hrs	Loss of ability to record and analyse Performance & Capacity data The service will not be available until the fail-over to a spare Blade is completed **Minimal Impact: Fujitsu Services**	Resolve via Incident Management

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
54.	Branch Support Database Server (BRS)	Loss of the server in IRE11 - No secondary server	0	8 hrs	Loss of ability to access the Branch Support database by support teams The service will not be available until the fail-over to a spare Blade is completed **Impact: Fujitsu Services**	Resolve via Incident Management
55.	Network Management System (NMS)	Loss of a single system in IRE11 or IRE19	1	8 hrs	Loss of ability to monitor the network from one data centre **Minimal Impact: Fujitsu Services**	Resolve via Incident Management Access the NMS in the alternative Data centre

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
56.	Network Management System (NMS)	Loss of both systems - IRE11 or IRE19	0	2 hrs	Loss of ability to monitor the network using the NMS tools **Impact: Fujitsu Services**	Resolve via Incident Management SMC and Network Support team would use other monitoring tools such as Tivoli to provide a reduced level of monitoring
57.	Primary & Secondary Campus – Network Infrastructure	Vodafone Data Network Service Failure of primary and secondary exchanges. (ADSL IP Data)	0	Immediate	General HNGX Services via the Vodafone Data Network **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. **HNGX Services MBCI Trigger** **Inform: POL BCT**
58.	Primary & Secondary Campus – Network Infrastructure	Fujitsu Services single POP failure. (ADSL IP Stream)	1	4 hrs	General HNGX Services via the IP Stream Network **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. Ensure Fujitsu Core Services switch to the secondary POP. **HNGX Services Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
59.	Primary & Secondary Campus – Network Infrastructure	Fujitsu Services Dual POP failure. (ADSL IP Stream)	0	Immediate	General HNGX Services via the IP Stream Network **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. **HNGX Services MBCI Trigger** **Inform: POL BCT**
60.	Primary and Secondary Campus – Network Infrastructure	Dual FJS Core ISP Satellite LNR router failure	0	Immediate	All BT VSAT Branches (approximately 60) will lose communications with the Fujitsu Services Data-centres. **Business Impact: POL**	This equipment is supplied and managed by FJS Core ISP Resolve via Incident Management **HNGX Services MBCI Trigger** **Inform: POL BCT**
61.	Network (To Outlets)	Satellite Service Failure. Loss of BT equipment at Turin.	1	Immediate	Loss of online services for 1 or more BT VSAT Branches **Impact: , Fujitsu Services, POL**	Resolve via Incident Management **MBCI Trigger** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
62.	Network (To Outlets)	ISDN BT Tail Loss of network connection to individual outlets	2	Immediate	General HNGX Services **Minimal Impact**	Resolve via Incident Management **(Refer to Appendix One for Outlet MBCI Triggers)**
Site Specific Buildings & People						
BRA01						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
63.	Fujitsu Services (POA) Bracknell site	Unavailable through fire/flood/bomb/ industrial action/ unspecified disaster	0	Immediate	Unable to provide any Bracknell based services. Impact: Fujitsu Services, POL	After obtaining confirmation from the BRA01 incident controller that it is a genuine fire or disaster invoke Business Continuity and relocate provision of services to LEW02 EMS keep a reserved and separate stock for Fujitsu of 60 laptops (20 each at MAN35 / STE04 / BRA01) built and ready to deploy (apart from the personalisation) for DR contingency. **MBCI Trigger** **Inform POL BCT**
64.	Fujitsu Services (POA) Bracknell site - building	Mains power unavailable / interrupted	1	36 hrs	**No Impact**	Power supply maintained by UPS and backup generator
65.	Fujitsu Services (POA) Bracknell - building	UPS non functioning	1	36 hrs	Unscheduled closedown of all systems and equipment. Minimal Impact.	Backup Generator powered up. All systems restarted to provide capability

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
66.	Fujitsu Services (POA) Bracknell - building.	Total power loss including backup generator Unavailable and/or non functioning	0	Immediate	Unable to provide any Bracknell based services. **Business Impact: Fujitsu Services POL**	Invoke Business Continuity and relocate provision of Ref. Data service to LEW02 **Potential MBCI Trigger** **Inform POL BCT**
67.	Fujitsu Services (POA) Bracknell - building	Air conditioning failure	1	4 hours	Equipment overheating leading to unscheduled closedown. No ability to change Reference Data, software fixes. No ability to progress diagnosis of software problems. Minimal Impact	Resolve problem via maintenance contract. Switch off non-essential equipment and instigate the immediate hire of cooling units.
68.	Fujitsu Services (POA) Bracknell - building	Telephone system unavailable	1	1 hour	No ability to receive incoming calls or faxes. Minimal Impact	Use mobile phones.
69.	Fujitsu Services (POA) Bracknell site - network	IP Select (CE or PE) single Wide Area Network router failure	1	8 hours	No Impact.	Failure resolved using normal support routes. Alternative network access achieved via LEW02 and/or IRE11 route. Possible degradation in response times

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
70.	Fujitsu Services (POA) Bracknell site - network	IP Select (CE or PE) Dual Wide Area Network routers failure	2	8 hours	No Impact.	Failure resolved using normal support routes. Alternative network access achieved via LEW02.Possible degradation in response times
71.	Fujitsu Services (POA) Bracknell site - network	Bracknell to LEW02 network router failure	2	8 hours	No Impact.	Failure resolved using normal support routes. Alternative network access achieved automatically via IRE11/IRE19 route. Possible degradation in response times.
72.	Fujitsu Services (POA) Bracknell site - network	Bracknell to LEW02 network circuit failure Vodafone IP Select network	2	8 hours	No Impact.	Failure resolved using normal support routes. Alternative network access achieved automatically via the remaining Vodafone IP Select link. Possible degradation in response times.
73.	Fujitsu Services (POA) Bracknell site	LST rig components failure	2	24hrs	Potential unscheduled interruption to testing.	Replacement sourced from spare equipment holding. Rebuild from scratch using build scripts

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
74.	Fujitsu Services (POA) Bracknell site	BIM System corruption	1	24 hrs	Manual recording of incidents. (POL have copies of previous BIM reports which are published on a daily basis) Minimal Impact	REC team to restore from backup. Provide paper BIM notes as applicable. (REC team have previously taken to a corporate network drive and provide paper BIMS as applicable)
75.	Fujitsu Services (POA) Bracknell site	Total loss of MIS IT infrastructure (MIS client)	0	24 hrs	No impact	Resolve via incident management MIS can use either their laptops via SSN or relocate to STE04 where there is another MIS client
76.	Fujitsu Services (POA) IRE19	Total loss of LST IT infrastructure	0	24 hrs	**Minimal Impact**	A hot Standby LST rig is available in LEW02
77.	Fujitsu Services (POA) Bracknell site	Total loss of SSC IT infrastructure	0	Immediate	**Minimal Impact**	SSC may invoke DR using remote working lap tops. Warm standby workstations are also available at LEW02.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
78.	Fujitsu Services (POA) Bracknell site	Failure of the Primary PEAK Incident Management Server	1	8 hrs	Minimal Impact	Resolve via Incident Management. Invoke Secondary Peak Server at LEW02
79.	Fujitsu Services (POA) Bracknell site	Total loss of RDT IT infrastructure	0	24 hrs	There is no immediate impact due to the loss of Ref. Data IT Infrastructure. **Impact: Fujitsu Services POL**	Invoke Business Continuity and relocate provision of Ref. Data service from LEW02 Note RDMC Admin Workstation is available in STE04 **Potential MBCI Trigger** **Inform POL BCT**
80.	Fujitsu Services (POA) Bracknell site	Failure of one POL e-mail laptop	2	N/A	Minimal Impact.	Use one of the other mailboxes.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
81.	Fujitsu Services (POA) Bracknell site	Failure of all laptops or POL e-mail service	1	24 hrs	Inability to receive/transmit requests/authorisations etc to/from POL. Minimal Impact.	Revert to fallback facilities, e.g. telephones, floppy disc, fax, etc. EMS keep a reserved and separate stock for Fujitsu of 60 laptops (20 each at MAN35 / STE04 / BRA01) built and ready to deploy (apart from the personalisation) for DR contingency.
82.	Fujitsu Services (POA) Bracknell site	Failure of one RDMC workstation	1	N/A	**No Impact.**	Use one of the other workstations. A Hot standby RDMC workstation is available in LEW02.
IRE11/ IRE19						
83.	FSCS SOS Operations IRE11	Failure of primary KMS Admin Workstation (IRE11)	1	8 hrs	**No Impact**	Resolve via Incident Management Use the secondary Admin Workstation at IRE19
84.	FSCS SOS Operations IRE11	Failure of primary Wide Area Network Router. (IRE11)	1	4 hrs	**No Impact**	Resolve via Incident Management Use the secondary Wide Area Network Router.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
85.	FSCS SOS Operations IRE11	Failure of both Wide Area Network Routers. (IRE11)	0	2 hrs	**No Impact**	Resolve via Incident Management Use the secondary Admin Workstation at IRE19 (Belfast).
86.	FSCS SOS Operations IRE11	Failure of both KMS Admin Workstations and/or WAN routers at both IRE11 and IRE19.	0	1 hr	**No Impact**	Resolve via Incident Management If required relocate appropriate SOS Staff to IRE11, BRA01 or LEW02
87.	IRE11 to POA Network	Single Router Fail	1	4 hrs	**No impact**	Resolve via Incident Management. Use alternative router
88.	IRE11 to POA Network	Dual Router Fail	0	1 hr	Loss of network communications from IRE11, no direct system management possible **Impact:**	Resolve via Incident Management. Temporary support can be provided by staff based at sites other than IRE11 Relocate support staff to IRE19 **Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
89.	Access to IRE11	Total loss of access for any reason	1	1 hr	No direct system management possible **Impact:**	Resolve via Incident Management. Temporary support can be provided by staff based at sites other than IRE11 Relocate support staff to IRE19 **Potential MBCI** **Inform: POL BCT**
90.	IRE11 Data Centre – Production Site	Total or substantial loss of the services for any reason (fire/flood/storm etc)	0	Immediate	Loss of all services from IRE11 - All service affected. **Major Impact: Fujitsu Services / POL**	Resolve via Incident Management/Fault procedure. If no possibility of restoring full service within 30 mins then full site failover to IRE19. May need to relocate support staff to IRE19 **MBCI Trigger** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
91.	IRE11 Data Centre Air Conditioning	Air conditioning – loss of 50% or more of capacity	0	Immediate	Kit overheating, higher potential for equipment failures Major Impact: Fujitsu Services / POL	Resolve via Incident Management/Fault procedure. Consider use of portable Air Con units. Consider failover to IRE19 data centre. Review switching off any non-essential equipment. **Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
92.	IRE11 Data Centre Power	Total Mains Power failure from all sources.	0	4hrs	Potential loss of all services Minimal Impact.	Resolve via Incident Management/Fault procedure. Power to the site is drawn from two separate sources on the grid. If one fails the other will take the load. Additional resilience is provided by UPS and generators. Ensure UPS and generators switch in. **Potential MBCI** **Inform: POL BCT**
93.	IRE11 Data Centre Power	Backup generator test failure	1	24 hrs	No resilience in total power loss scenario. **No impact** (Assuming mains power still available.)	Resolve via Incident Management/Fault procedure.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
94.	IRE11 Data Centre Fire/Flood Detection Systems	Fire/Flood Detection System failure	1	8 hrs	Loss of monitoring only. No loss of service – small increased risk **No Impact**	Resolve via Incident Management/Fault procedure.
95.	IRE11 Data Centre Building Security Systems	Security systems CCTV malfunction	1	8 hrs	Loss of monitoring only. No loss of service – small increased risk **No Impact**	Resolve via Incident Management/Fault procedure.
96.	IRE19 Data Centre – Part Production / DR / Test site	Total or substantial loss of the services for any reason (fire/flood/storm etc)	0	Immediate	Loss of all Live services from IRE19. All live services can run from IRE11 Loss of all test & development services No failover / DR site available **Impact: Fujitsu Services / POL**	Resolve via Incident Management/Fault procedure. **MBCI Trigger** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
97.	IRE19 Data Centre Air Conditioning	Air conditioning – loss of 50% or more of capacity	0	Immediate	Kit overheating, higher potential for equipment failures **Major Impact: Fujitsu Services**	Resolve via Incident Management/Fault procedure. Consider use of portable Air Con units. Review switching off any non-essential equipment.
98.	IRE19 Data Centre Power	Total Mains Power failure from all sources.	0	4hrs	Potential loss of all test services Impact. Fujitsu Services	Resolve via Incident Management/Fault procedure. Power to the site is drawn from two separate sources on the grid. If one fails the other will take the load. Additional resilience is provided by UPS and generators. Ensure UPS and generators switch in. **Potential MBCI** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
99.	IRE19 Data Centre Power	Backup generator test failure	1	24 hrs	No resilience in total power loss scenario. **No impact** (Assuming mains power still available.)	Resolve via Incident Management/Fault procedure.
100	IRE19 Data Centre Fire/Flood Detection Systems	Fire/Flood Detection System failure	1	8 hrs	Loss of monitoring only. No loss of service – small increased risk **No Impact**	Resolve via Incident Management/Fault procedure.
101	IRE19 Data Centre Building Security Systems	Security systems CCTV malfunction	1	8 hrs	Loss of monitoring only. No loss of service – small increased risk **No Impact**	Resolve via Incident Management/Fault procedure.
IND49/ IND46						
102	SMC - IND49 building	Any total loss of use by off-shore SMC, e.g., loss of building, network connections, etc.	1	> 1hr	The service(s) provided from the building are severely disrupted or terminated **Impact: SMC / Fujitsu Services**	Invoke SMC off-shore site contingency plan. Some services can be provided by MSS/ SSC. **MBCI Trigger** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
103	GDC Development – IND49 building	Any total loss of use by off-shore development, e.g., loss of building, network connections, etc.	1		Extremely unlikely as we run a blended service model so at any point there will be Indian guys in the UK (3-4) working alongside UK resources with the same skill-set. Development data is copied between sites.	No formal DR requirement. Resolve via incident management.
104	People SMC (IND49)	Any total loss	0	>	Extremely unlikely since staff work on shifts – 2nd line support, system monitoring, software distribution capability lost **Impact: SMC, Fujitsu Services**	Invoke SMC off-shore contingency Plan. Some services can be provided by MSS / SSC. **MBCI Trigger** **Inform: POL BCT**
105	GDC Development Team People (IND49)	Any total loss	0		Extremely unlikely as we run a blended service model so at any point there will be Indian guys in the UK (3-4) working alongside UK resources with the same skill-set.	Resolve via incident management.
BLA01						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
106	Buildings Blackpool BLA01 (MSS North, SMG)	Total loss for any reason	0	> 1 hr	The service(s) provided from the building are severely disrupted or terminated. **Impact: MSS, SMG, Fujitsu Services**	Staff can work from home or WAR07 **MBCI Trigger** **Inform: POL BCT**
107	MSS / SMG people BLA01	Any total loss	0	> 1 hr	Extremely unlikely since staff work on shifts and from home - 3rd line support and development capability lost **Impact: MSS, SMG, Fujitsu Services**	Invoke SMG/MSS contingency plan. Some services can be provided by 4LS/ SSC. **MBCI Trigger** **Inform: POL BCT**
WAR07						
108	Buildings Warrington WAR07 (POA Networks)	Total loss for any reason	0	> 1 hr	The service(s) provided from the building are severely disrupted or terminated. **Impact: POA Networks, Fujitsu Services**	Staff can work from home or BLA01 **MBCI Trigger** **Inform: POL BCT**
CRE02						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
109	Buildings Crewe CRE02 (OBC)	Total loss for any reason	0	> 12 hr	There may be a delay to processing OBC queries. **Impact: OBC, Fujitsu Services**	One team member's OBC laptop can be used to work from home. Resolve via incident management
Miscellaneous						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
110	Buildings	Loss of one or more major building.	0	Immediate	The service(s) provided from the building are severely disrupted or terminated **Impact: , Fujitsu Services, POL**	Invoke Major Site Contingency Plan EMS keep a reserved and separate stock for Fujitsu of 60 laptops (20 each at MAN35 / STE04 / BRA01) built and ready to deploy (apart from the personalisation) for DR contingency. **MBCI Trigger** **Inform: POL BCT**
111	People	Loss of staff at one or more locations.	0	Immediate	The service(s) provided by a team are severely disrupted or terminated **Impact: POL**	**MBCI Trigger** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
112	Phone System	Failure of corporate landline telephones, for any reason	1	Immediate	**No impact**	Resolve via Incident Management. Use mobile phones or OCS as required
113	Phone System	Failure of corporate mobile telephones, for any reason	1	Immediate	**No impact**	Resolve via Incident Management. Use landline telephones, personal telephones or OCS as required
114	Collaboration	Complete loss of SharePoint	1	48 hours	Inability to access Major Incident Reports	Refer to mailboxes where reports were sent
115	Collaboration	Complete loss of ProjectWeb	1	48 hours	Some NT work instructions unavailable may mean certain incident resolutions may be slower.	Additional support provided by system owners where required.
116	Document Management	Complete loss of PVCS	1	4 hours	Inability to access Change Proposals and their associated documents	Resolve via incident management. Consider failing over to LEW02
117	Document Management	Complete loss of Dimensions	1	4 hours	Inability to view/edit the official store of HNG-X documentation	
VODAFONE (Cable & Wireless)						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
118	VODAFONE ISDN2 not available for new Post Office	New Post Office Provision	1	45 days	Minimal, Post Office able to continue working. **Impact: POL**	Resolve via Incident Management. VODAFONE to provide alternative solution, e.g. satellite.
119	VODAFONE National Number Change	Fujitsu Services Data-centre routers	1	6 months	Parallel running of old and new numbers. Impact: Fujitsu Services, POL, VODAFONE	Resolve via Incident Management. Fujitsu Services to reprogram data-centre routers for new numbers.
120	VODAFONE Data-centres to VODAFONE network	Switch/SNAP/fibre fail	2	5 hrs	Resilience designed into solution. **No impact.**	Resolve via Incident Management. Use alternative routes
121	VODAFONE Post Offices into VODAFONE network	ISDN2 fail/ BT LSE fail	3	2 days	Minimal, Post Offices able to continue working. **Impact: POL**	Resolve via Incident Management. VODAFONE CCC fault reporting process.
122	VODAFONE Network congestion issues (ISDN network)	VODAFONE and or BT Network	3	1 day	Slow data transfer. **Impact: , Fujitsu Services**	Resolve via Incident Management. VODAFONE and BT traffic monitoring – traffic re-routes instigated.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
123	VODAFONE Network congestion issues (VODAFONE data network)	VODAFONE IP Select Network	3	4 hrs	Slow data transfer. **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. VODAFONE monitoring – traffic re-routes instigated.
124	VODAFONE Bracknell NMC unavailable e.g. bomb/fire	VODAFONE, Bracknell Network Management Centre	0	1 hr	A NMC disaster recovery site is available at Watford. **Impact: , Fujitsu Services, POL**	Resolve via Incident Management. VODAFONE Disaster recovery processes. **Potential MBCI** **Inform: POL BCT**
125	VODAFONE Evacuation of BT SMC	BT SMC	0	1 hr	**Impact: VODAFONE**	Resolve via Incident Management. BT DR document
126	VODAFONE FSCS change process	New Post Office Provision	2	45 days	VODAFONE require 45 working days notice to provide ISDN service to a new Post Office. **Impact: POL**	Resolve via Incident Management. change control document.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
127	VODAFONE ISDN2 not available for new Post Office	New Post Office Provision	1	45 days	Minimal, Post Office able to continue working. **Impact: POL**	Resolve via Incident Management. VODAFONE to provide alternative solution, e.g. satellite.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

11 Risks Identified Against Major Account Controllers (MAC)

The table below summarises the identified risks to the provision of the MAC services.

As a matter of normal operational practice, a call would be placed against MAC (or other Fujitsu Services support unit) if any of the identified risks materialised.

The intention is that the list identified can act as a guide to personnel assessing and managing any significant incident affecting the MAC.

The table within section contains a column identified as probability with a range of 0 to 4. These estimate the probable risk of failure. It must be emphasised that these are not percentages and should be considered simple weighting factors.

The probability of failure of major elements of the service is low because:

1. There has been a high level of resilience and duplication built into the infrastructure.
2. Extensive validation has been performed upon the infrastructure.

11.1 Trigger Tables for Major Account Controllers (MAC)

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
1.	BT telephone call delivery system via SPoC IVR system	Any failure by BT lines into SpoC (at POL)	1	Immediate	Total loss of MAC service Possible SLT Failure Possible Business Impact: POL, Fujitsu Services, MAC tesm	(100% service requirement placed on BT via resilient systems, links contracted to POL not Fujitsu Services, therefore no contingency possible within Fujitsu Services) Log test calls / investigate Resolve via MAC incident process Consider site relocation for some staff to the DR site, and invoke fourth floor desk clearing process if required. **MBCI Go to 10.2.1** **Inform: POL BCT**
2.	Commander\ ACD telephone call management system – STE04	Partial loss. Loss of Commander with failover to ACD.	2	Immediate	5 minute loss of telephony while system fails over. Ability to monitor and manage queues lost **Minimal Impact**	Issue ACD Pins to agents. Use ACD system until Commander restored. (See section 10.2.6) Resolve via MAC incident management process.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
3.	Commander\ ACD telephone call management system – STE04	Total loss for any reason.	1	Immediate	**Major Impact** NO calls being taken **Potential Business Impact on HSD and Fujitsu Services, POL**	**For HSD:** See section 4.2 UPS would provide emergency, then a generator would provide power. Invoke BT Command Link to switch to voicemail & put message on IVR via NBSC Resolve via HSD incident process > 60 mins consider temp site relocation to DR site in BRA01, and invoke fourth floor desk clearing process if required. **MBCI Go to 10.2.2** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
4.	Loss of access to TIVOLI at STE04 HSD	Any failure Total Loss	1	< 1 hr > 1 hr	**Minimal Impact**: HSD - No ability to handle calls that require ability to access a PO Counter system Probable SLT failure **Major Impact** **Business Impact:** **HSD, Fujitsu Services, POL**	Resolve via incident management process. Request MSS & SMC to assist. **Potential MBCI Go to 10.2.5** **Inform: POL BCT**
5.	Voicemail failure for OOH calls	Any failure	0	> 8 hrs	Call volumes very low Out Of Hours, unless a major problem is encountered, or is anticipated **Minimal Impact:** **HSD, POL**	Unknown until next day for normal operation Resolve via incident management process **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
6.	STE04 HSD site non-operational	For any reason HSD lost of 100% capacity for all HSD activities	1	< 30mins > 20mins	**Minimal impact** **Major Impact.** Call queuing No calls being taken by HSD Probable SLT failure if over an extended period. **Business Impact:** **HSD, Fujitsu Services and POL**	**For HSD:** Invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and Fujitsu Services Data Centres. Consider relocation to DR site in BRA01, and invoke fourth floor desk clearing process if required. Resolve via HSD incident process. **MBCI Go to 10.2.2** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
7.	Loss of people in STE04 - HSD	Loss of access to most staff	0	< 20mins > 20mins	**Minimal Impact** **Major Impact.** No calls being taken by HSD Call queuing Probable SLT failures **Business Impact:** **HSD, Fujitsu Services and POL**	**HSD** must invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and Fujitsu Services Data Centres. Resolve via HSD incident process. **MBCI Go to 10.2.3** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
8.	TRIOLE Incident Management System	Partial failure	2	> 8 hrs	**Minimal Impact** Possible slower response times Loss of resilience whilst restoration to normal service is being performed. **Minimal Business Impact:** **HSD**	All users that were logged into the failed server will need to log in to the remaining server Resolve via HSD incident management process.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
9.	TRIOLE Incident Management System	Total loss for any reason	1	Immediate	**Major Impact:** Unable to log calls quickly. Possible queuing if calls levels high. Possible SLT failure if over an extended period. **Potential Business Impact: HSD, Fujitsu Services and POL**	Implement Manual Call Logging Resolve problem via HSD incident management process. **Potential MBCI Go to 10.2.4** **Inform: POL BCT**
10.	Loss of One Shot Password workstations in STE04	Any circumstances All OSP workstations unavailable Lost 100% capacity	0	< 1 hr > 1 hr	**Minimal Impact:** Unable to resolve some outlet problems **Major Impact** **Potential Business Impact: HSD / POL / FMS**	Resolve via HSD incident management process 6 One Shot Password workstation available for contingency Consider using the 2 DR one Shot Password workstations in BRA01

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
11.	TRIOLE Incident Management System to D1 OTI link	Any failure Automated process lost	2	> 4 hrs	**Minimal Impact:** **HSD / FMS** (Unless over an extended period with high call volumes)	Resolve problem via HSD incident management process. E-mail or Fax details or hand carry call details that would be passed into D1 to FMS Service Desk
12.	Incident Management System to Peak link	Any failure Automated process lost	2	> 4 hrs	**Minimal Impact:** **HSD Fujitsu Services Support services** (unless over an extended period)	Resolve problem via HSD incident management process. Fax details of calls that would be passed into Peak to the SSC.
13.	POA Network link(s) to both Data-centre(s)	Any failure to both sites (IRE11 & IRE19)	0	> 30 mins	No access to Tivoli (see Risk 3) **Business Impact:** **HSD, Fujitsu Services, POL**	Resolve via incident management process. Alternate network routes make this unlikely. Request MSS & SMC to assist. **Potential MBCI Go to 10.2.5** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
14.	Loss of Corporate Network	For any reason in STE04	1	Immediate	HSD unable to access TRIOLE Incident Management System and other services. This will slow call resolution. Unable to fully verify caller details. Loss of e-mail. Possible SLT failures for HSD Business Impact: HSD, Fujitsu Services, POL	Invoke Manual call logging process. Resolve via problem management process. Consider relocation to DR sites if BRA01 site is unaffected,, and invoke fourth floor desk clearing process if required. **Potential MBCI Go to 10.2.4** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
15.	Loss of Corporate Network	For any reason At SDC01	1	Immediate	HSD unable to access TRIOLE Incident Management System and other services. This will slow call resolution. Unable to fully verify caller details. Loss of e-mail. Possible SLT failures for HSD Business Impact: HSD, POL	May be possible to access TRIOLE via another data centre server, otherwise invoke manual call logging process. Resolve via problem management process. **Potential MBCI Go to 10.2.4** **Inform: POL BCT**

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
Major Account Controllers (MAC)						
16.	Loss KMA functionality	Total loss of all KMA workstations in STE04 for any reason	1	< 2 hrs > 2 hrs	**Minimal Impact:** Unable to resolve some outlet problems **Major Impact** **Potential Business Impact: HSD / POL / FMS**	Resolve via HSD incident management process There are 7 workstations in STE04 for contingency Consider using the KMA workstations in BRA01

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

12 Summary of Contingency Actions

12.1 Summary of Contingency Actions for HNG-X Support Services

The following are additional contingency actions to be taken for the risks identified in the table in section 11.2.

12.1.1 Reconciliation Service

There are many essential systems that enable the Reconciliation Service to continue operating. These include BIMS database, TWS schedule (successful run), Delivery of reports, TES, DRS, APS. Contingency actions to be defined.

12.1.2 Security Management Service

To be defined

12.1.3 Branch Change Management Service

To be defined

12.1.4 Estate Management Service

To be defined

12.1.5 Network Services

To be defined

12.1.6 Data Centre Operations Service

To be defined

12.1.7 SAP Development and QA-Test Systems

No further actions

12.1.8 System Management Service

To be defined

12.1.9 Support Services

To be defined

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

12.1.10 System Operate Services

To be defined

12.1.11 Reference Data Management Service

To be defined

12.1.12 Service Integration Service

No further actions

12.1.13 Receipt Template Service

No further actions

12.1.14 Service Management Service

To be defined

UNCONTROLLED IF PRINTED

12.2 Summary of Contingency Actions for the MAC

The following are additional contingency actions to be taken for the risks identified in the table in section 12.1.

12.2.1 BT Telephone Call Delivery System, via IVR (NBSC), to MAC.

There is no contingency action to be performed by MAC over and above normal operational incident processes and the actions identified within the above risk tables. This is a BT supplied service.

12.2.2 Loss of Functionality in STE04 for MAC

If STE04 (the primary site in Stevenage) is unavailable for use by MAC provision has been made for staff to re-locate to facilities in BRA01, another Fujitsu Services site in Bracknell. If BRA01 disaster recovery site is invoked the POA Duty Manager is to arrange that all staff occupying MAC DR desks on the fourth floor are instructed that they are to be vacated.

In addition a provision has been made to allow phone contact to be re-established once staff have relocated, via a BT command switch. During any period when MAC is unavailable to take calls, the calls will be directed to the voicemail service. Once staff are operational at the alternate location the voicemail calls will be processed and the callers will be called back. There is about one hundred desktop PCs in STE04 that can be used for TfS, and other related services , and forty laptops in BRA01.

12.2.3 People

© Copyright Fujitsu Services Limited 2014

FUJ00232658

Human Resource Management processes are in place to manage the normal turnover of staff.

12.2.4 Manual Processes due to total loss of TfS Incident Management System

In the event that the TfS servers have failed at both SDC01 and SDC02, or are inaccessible, or are in the processed of being failed over, manual processes will be used to log calls until such time as TfS can be returned to service.

12.2.5 Loss Of access to Tivoli / KMA / Global User Counter / One Shot Password System

In the event of the unavailability of Tivoli at STE04, including and PCs used by the SMC, for an extended period of time (at least 3 hours) then temporary relocation to BRA01 shall be considered. There are twenty five Tivoli PCs in STE04 and four at the DR site in BRA01.

In the event of the unavailability of all of the KMA (Key Management) Workstations (there are seven in STE04 – and one in BRA01), or all One Shot Password Systems in STE04 (there are six in STE04 - two in BRA01). for an extended period of time (at least 3 hours) then temporary relocation to BRA01 shall be considered in order to provide this capability.

12.2.6 Loss Commander – Call Management

In the event that calls are not being passed by the normal call management system (Commander) it is possible to switch to the use of the standard ACD (Auto Call Distribution) system, however this may limit call management capability and reduce the number of calls being handled.

If whatever has caused the Commander system to be unusable is also preventing use of the ACD system then calls will be diverted to voice mail and consideration given to a moving to the DR site.

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

13 Post Office Limited failures impacting POA Services

13.1 Post Office Limited failures impacting POA RDMS Service

The POA RDMS utilises Reference Data being supplied by POL Chesterfield but is not strictly dependent on it. It is the POL business which is dependent on the data.

The availability of Post Office outlets to utilise the RDMS to the customer is a further prerequisite of the end to end service provision.

13.2 POL and AP Client failures impacting POA APS Service

13.2.1 Post Office Limited

The availability of Post Office outlets to provide the Automated Payment Service to the customer is a further prerequisite of the end to end service provision.

Non-availability of one or more post Office outlets restricts the availability of the service and may trigger a Business Continuity event, see Appendix One.

13.2.2 AP Clients

The availability of the Automated Payment Clients to receive the transaction files is a further prerequisite of the end to end service provision.

Non-availability of one or more of the AP Clients restricts the availability of the service and may trigger a Business Continuity event.

The Fujitsu Services POA plans and procedures for dealing with this situation can be found in the Client Specific Operational Level agreements (CS/OLA/003 – Generic AP Client OLA from which all specific Client OLA's are derived).

UNCONTROLLED IF PRINTED

13.3 Post Office Ltd failures impacting POA TPS Service

Non-availability of TPS service at POL NDC, or the disaster recovery site at Isleworth, or one or more Post Office outlets restricts the availability of the service and may trigger a Business Continuity event, see Appendix One.

13.4 Post Office Ltd and Supplier failures impacting POA NBS Service

The non-availability of one or more of the Financial Institutions or one or more Post Office outlets can restrict the availability of the Network Banking Service and may trigger a Business Continuity event

13.5 Post Office Ltd and Supplier failures impacting POA DCS Service

The non-availability of the Streamline Debit Card System, or one or more of the Card Issue services, or one or more Post Office outlets can restrict the availability of the Debit Card Service and may trigger a Business Continuity event.

© Copyright Fujitsu Services Limited 2014

FUJ00232658

14 Plan Activation

14.1 Major Business Continuity Incident (MBCI)

Once the criteria for Business Continuity have been satisfied, i.e. an MBCI Trigger from the table of risks in section 10 & 12 Impact & Risk Assessment then after a call had been placed and appropriate details logged at MAC, the problem ownership is passed to the Fujitsu Services POA member of the BCMT (Business Continuity Management Team)

After compiling all relevant information, and if necessary communicating this to the other members of the BCMT listed below in the Contact List, a full impact assessment will be conducted to determine if the joint Business Continuity Management Processes detailed in:

CS/PRD/031 (Fujitsu Services (POA) Business Continuity Management) and

SVMSDMSIP0001 (Post Office Limited and Fujitsu Services Business Continuity Interface Agreement) will be invoked.

This will be done in conjunction with Senior Managers, relevant Business Units and Expert Domains as appropriate

If the Joint BCM processes are invoked, the next steps will be to agree who from the BCMT owns the MBCI.

The BCMT will then agree a plan of action and agree upon the recovery and contingency activities to be carried out. Again, this will be done in conjunction with Senior Managers, relevant Business Units and Expert Domains as appropriate.

The agreed plan will then be monitored and reviewed until such time as the MBCI (Major Business Continuity Incident) impacting the service has been resolved, and the MBCI closed.

14.2 Site Failover

Site failover is covered by a Major Incident Process.

Some of these steps will be capable of being carried out in parallel. Major checkpoints will be included in the business continuity plan to allow coordination of steps which depend on each other.

Testers will be given as much notice as possible to stop their testing and shut down their systems cleanly.

A message will be put on the MAC team phone to inform Post Masters and Mistresses of a major problem

Authorisation will be sought for failover

Availability and operation of support services will be confirmed.

If possible production servers and LPANs at the primary site will be shut down cleanly, followed by Test LPANs at the secondary site.

The test network will be disabled and the production network prepared for operation from the secondary site

The storage will be failed over.

The Production LPANs will be started at the secondary site

Business critical services will be started

Other services will be started

States of sites - IRE11 Primary / IRE19 Secondary:

Normal Running:

UNCONTROLLED IF PRINTED

FUJ00232658

Primary – Production

Secondary – Test/Production*

After Disaster:

Primary – non-functional / unavailable

Secondary – Test/Production*

After Failover:

Primary – Unavailable

Secondary – Production / Limited Test

After Failover and after primary site fault is fixed:

Primary – Standby

Secondary – Production / Limited Test

* The bulk of the Secondary data centre is used as a test environment

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

15 Contact List

15.1 Normal Processes

Organisation	Contact Name	Role	Telephone Number
POA	As per rota distributed by MAC team	Duty Manager Or Office Hours applicable Service Delivery Manager	Pager: GRO
	Peter Thompson	CS Head of Service Management	Mobile: GRO
(MBCI Contacts)	Changdev Pawashe	Business Continuity Manager	Mobile GRO
	Peter Thompson	CS Head of Service Management	Mobile GRO
FS Core Services	Roger Stearn	Network Manager	Mobile GRO Internal : GRO
FS Core Services SOS NT and UNIX	Adrienne Thompson	SOS NT and UNIX Manager	Office: GRO Mobile: GRO
FS Core Services SMC	Jacob Cherian	SMC Manager	Office: GRO Mobile: GRO
		Business Stream Manager	Office: GRO Mobile: GRO
Post Office Limited (ATOS)		ATOS IT Service Continuity management team GRO	

UNCONTROLLED IF PRINTED

15.2 Escalation Processes

Escalation Level	Level 1	Level 2	Level 3	Level 4
Fujitsu Services POA	Duty Manager Pager: GRO Or Office Hours	Problem Manager (Assigned by Duty Manager)	CS Security Operations Manager. Kumudu Amaratunga	Customer Service Operations Director. Peter Thompson

© Copyright Fujitsu Services Limited 2014

FUJ00232658

	applicable Day Time POA Duty Manager Via MAC team.	Business Continuity Manager. Changdev Pawashe Office: GRO Mobile: GRO GRO	Mobile: GRO	Mobile: GRO Chief Information Security Officer Keith Smith Mobile: GRO
FS Core Services **Networks** **SOS NT and UNIX** **SMC** **MAC Team**			Network Manager Mobile GRO Internal GRO NT&UNIX Manager Andrew Gibson Office: GRO Mobile: GRO SMC Manager Jacob Cherian Office: GRO Mobile: GRO MAC Ops Manager Sandie Bothick Mobile: GRO	Data Networking Support Manager POA Networks Duty manager – GRO Technical Support Manager Fiona Iennox Mobile: GRO Office: GRO
Post Office Limited			Business Continuity Manager ATOS IT Service Continuity management team GRO	Network Support Service Manager. ATOS IT Service Continuity management team GRO

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

16 APPENDICES

16.1 Appendix One: Post Office Outlet Trigger Table.

The following table provides guidance on identifying the severity and classification of incidents that have an adverse affect on Post Office outlets. All problems, which are an exception to the 'normal' incident profile and fit within any of the categories defined below should be escalated to the POA Business Continuity Manager for consideration.

Not Geographically Concentrated Outlets.	
Less than 200 outlets affected for less than 0.5 of a trading day	A problem
Less than 200 outlets affected for between 0.5 and 1 trading day	Potential MBCI
Less than 200 outlets affected for more than 1 trading day	Potential MBCI*
Between 200 and 800 outlets affected for less than 2 hours of a trading day	A Problem
Between 200 and 800 outlets affected for more than 2 hours but less than one trading day	Potential MBCI
Between 200 and 800 outlets affected for more than one trading day	Potential MBCI*
800 and more outlets affected	Potential MBCI*
Geographically Concentrated Outlets.	
Between 10 and 20 outlets affected for less than 0.5 of a trading day	A Problem
Between 10 and 20 outlets affected for between 0.5 and one trading day	Potential MBCI
Between 10 and 20 outlets affected for more than one trading day	Potential MBCI*
Between 20 and 100 outlets affected for up to 1 hour of a trading day	A Problem
Between 20 and 100 outlets affected for between 1 hour and 0.5 of a trading day	Potential MBCI
Between 20 and 100 outlets affected for more than 0.5 of a trading day	Potential MBCI*
More than 100 outlets affected	Potential MBCI*

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014

FUJ00232658

16.2 Appendix 2 IRE11 – IS Data Centre Information

Refer to: ISN000666 - IS Data Centre Specification - IRE11

Describes the environmental specification for the IRE11 Data Centre

16.3 Appendix 2 IRE19 – IS Data Centre Information

Refer to: Refer to: ISN000667 - IS Data Centre Specification - IRE19

Describes the environmental specification for the IRE19 Data Centre

UNCONTROLLED IF PRINTED

© Copyright Fujitsu Services Limited 2014