FUJ00079946

Document Title: POA Customer Service Major Incident Escalation Process

Document Type: Process Definition

Release: N/A

Abstract: This describes the POA Customer Service Major Incident Escalation Process

Document Status: APPROVED

Originator & Dept: Mike Warren - Service Transformation.

Internal Distribution: Peter Thompson, Carl Marx, Tony Wicks, Mike Woolgar, Dean Felix, Ian Daniel, Julie Welsh, Graham Mockridge, Mick Lait, Mike Warren, Deirdre Conniss, Andy Gibson, Mik Peach, Dave Jackson, John Flannigan, Joep Niens, Rosemary Burgess, Nikki Hawkins, Mike Stewart, Nick Crow, Alex Kemp, Denise Miller, Dave Wilcox, Ian Mills, Kirsty Walmsley, Ian Cooley

External Distribution: Dave Hulbert (POL), Richard Ashcroft (POL)

Approval Authorities: (*See PA/PRO/010 for Approval roles)*

Name	Role	Signature	Date
Dave Baldwin	Director Customer Services		
Carl Marx	Service Management Team Manager		

FUJ00079946

0.0 Document Control

0.1 Document History

Version No.	Date	Reason for Issue	Associated CP/PEAK/PPRR Reference
0.1	02/05	First draft – to detail the baseline Incident Escalation process	
0.2	03/05	Draft to incorporate new organisation, trigger information and to mirror POL Incident and Problem Management Process Profile.	
0.3	05/05	Updated to reflect comments received.	
0.4	09/06	Updated - second round of comments	
1.0	01/07	Issued for approval.	

0.2 Review Details

Review Comments by:	[Date]
Review Comments to:	Mike Warren

Mandatory Review	
Role	*Name*
Service Management Team Manager	Carl Marx
Director Customer Services	Dave Baldwin**
Business Service Delivery Manager	Richard Brunskill
System Architect	Glenn Stephens
TDA	Simon Fawkes
TDA	David Tanner*
System Architect	Mark Jarosz
Optional Review	
Role	*Name*
FS CS Service Delivery Team Manager	Nikki Hawkins*
FS CS Support Delivery Team Manager	Peter Thompson*
FS CS Transformation Manager	Graham Mockridge
FS CS Business Continuity Manager	Tony Wicks**

FUJ00079946

FS CS Service Delivery Manager DataTransfer	Ian Daniel*
FS CS Service Delivery Manager Engineering	Dean Felix*
FS CS Service Delivery Manager BankOnLine	Mike Stewart
FS CS Service Delivery Manager HSD	Julie Welsh*
FS CS Service Delivery Manager BankOnLine	Mike Woolgar**
FS CS System Support Centre Manager	Mik Peach**
FS CS Operations Manager	Mick Lait*
Head of Call Centres Commercial & PS	Martin Croucher
Service Delivery Manager (Ops)	Ian Cooley*
Senior Consultant	Deirdre Conniss**
Unix Team Leader	Andy Gibson**
Northern Team Leader	Dave Jackson
Operations Manager	John Flanagan
Head of Data Centres	Joep Niens
Technical Support Manager	Rosemary Burgess
Data Networking Support Manager	Oyku Tevfik

(*) = Reviewers that returned comments

0.3 Associated Documents

Reference	Version	Date	Title	Source
PA/TEM/001			Fujitsu Services Document Template	PVCS
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	PVCS
CS/PRD/021			POA Problem Management Process	PVCS
CS/PRO/110			POA Problem Management Database Procedures	PVCS
PA/PRO/001			Change Control Process	PVCS
CS/QMS/001			Customer Service Policy Manual	PVCS
CS/SER/023			Horizon Service Desk –	Draft

FUJ00079946

			Service Description	
CS/PRD/074			POA Incident Management Process	PVCS
FJ/POA/NET/REF/076			Escalation Procedure IS/POA	PVCS
CS/FSP/002			Horizon System Helpdesk Call Enquiry Matrix and Incident Prioritisation	PVCS
CS/PRD/122			Major Incident Communication Process	PVCS
			SMS Messaging User Guide	PVCS
CS/PRD/121			SMS Major Communication Framework Process	Draft
CS/PLA/079			Horizon Services Business Continuity Plan	PVCS
CS/PLA/080			Horizon Support Services Business Continuity Plan	PVCS
CS/PLA/015			Horizon Systems Helpdesk and Business Continuity Plan	PVCS

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

N.B. Printed versions of this document are not under change control.

0.4 Abbreviations/Definitions

Abbreviation	Definition
HSD	Horizon Service Desk
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEL	Known Error Log
MSU	Management Support Unit
PO	Post Office
POA	Post Office Account
POL	Post Office Limited

FUJ00079946

SDMs	Service Delivery Managers
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
VIP	VIP Post Office, High Profile Outlet
A+G	Advice & Guidance
BCP	Business Continuity Plan
RFC	Request For Change
KEDB	Known Error Database
MBCI	Major Business Continuity Incident
SCT	Service Continuity Team
OCP	Operational Change Proposal

0.5 Changes in this Version

Version	Changes
1.0	For approval

0.6 Changes Expected

Changes
None

FUJ00079946

0.7 Table of Contents

FUJ00079946

1.0 Introduction

1.1 Process Owner

The owner of this process is the POA Service Delivery Team Manager.

1.2 Process Objective

The key objective is to improve the overall major incident management process as follows:

- Improvements within communication channels to become more effective and streamlined
- Improve accuracy of reporting against status of incident
- Allowing technical teams the right amount of time to diagnose and impact an incident
- Avoid unnecessary alerting of the customer
- Assessing which incidents are major and which are 'Business as Usual'
- Clarify the need to communicate awareness of potential incidents
- Demonstrate to the Post Office a more professional approach
- Provision of clear defined roles and responsibilities
- Defined reporting/update timelines through duration of a major incident.
- Improved governance

1.3 Process Rationale

This document outlines the communication and management process and guidelines to be followed in relation to Major Incidents impacting the live estate.

The methodology defined within this document augments the existing SMS framework process presently deployed within the live estate.

The aim of the document is to provide a pre-defined process on which future major incident communication and management will follow and that any parties involved in that process provide updates /receive updates at defined intervals from inception to closure of any major service impacts.

FUJ00079946

2.0 Mandatory Guidelines

Whilst it is important to maintain a balance between:

a) Allowing the technical teams the right amount of time to diagnose and impact an incident

b) Avoid unnecessary alerting of the customer

c) Assessing which incidents are major and which are 'Business as Usual'

The following guidelines should be adhered to.

- The Post Office Horizon Service Desk should be the first point of contact for operational contact between Fujitsu and the end user.
- The relevant technical teams who are monitoring and aware of a potential major incident must page/call the Fujitsu Service Delivery Manager (Duty Manager out of hours) as *soon as possible*, rather than wait. This is not limited to major incidents alone, but must be delivered wherever a state other than Business as Usual has been detected. The Fujitsu Service Delivery Manager must in turn communicate the potential incident, to their counterpart for awareness and monitoring in POL.
- The Fujitsu Service Delivery Manager (or Duty Manager out of hours) is responsible for communicating both *up* the Fujitsu Organisation and *across* (see appendix A) to their counterpart in POL. Where this is impractical (i.e. leave, out of hours, unavailable), the initiative should be taken to jump up the organisation. The important fact is that the customer is informed in a timely manner and at the correct touch point. This communication should be by voice or direct SMS. The communication should include the date, time, name, nature of problem, severity, if service affecting, and the owner for contact.
- The Fujitsu Service Delivery Manager should also initiate communication using SMS via HSD, 08.00 to 18.30 or via SMC 18.30 – 0800.

FUJ00079946

3.0 Definition of a Major Incident

3.1 Incident Classification

As a general rule a Major Incident will always be an incident rated as severity level A (critical) in the POA Customer Service Incident Management Process Details document (CS/PRD/074) version 3.0. However not all incidents rated at severity level A qualify. This is because the severity levels do not necessarily translate to the global business impact on POL's business. For example a single counter post office which is unable to transact, regardless of its business volumes is rated as a severity A.

For simplicity, Incidents are classified into three impact levels: High, Medium and Low.

High – An Incident that has occurred with a significant and potentially prolonged adverse impact on POL business. Typically these Incidents will initially require a significant amount of reactive management before they can be controlled and resolved.

Medium – An Incident that has the potential to cause significant impact to POL business but can be controlled and mitigated against through effective management.

Low – An Incident that requires business attention but if managed effectively will not have significant impact on POL business.

3.2 Influencing Factors

It is important that a major incident is defined as such because of its business impact on the day when it occurs, rather than simply being defined as a major incident because it appears on a list. The following parameters will also feed into the consideration of whether a major incident exists, as follows:

- Duration i.e. how long has the vulnerability to service already existed
- Impact across the estate, including consideration of whether a service is merely degraded or actually stopped
- Time at which the event occurs in relation to the 24 hour business day
- Anticipated time before service can be resumed
- Impact to POL Branches, customers, clients or brand image

FUJ00079946

3.3 Factors external to POL and POA

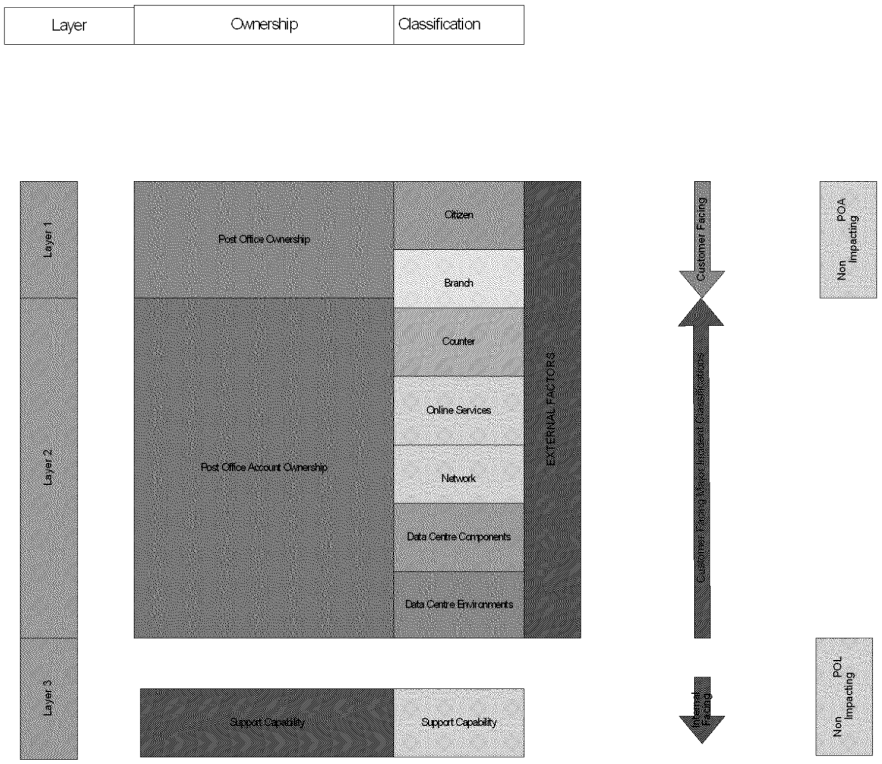
The following factors are external to both POL and POA and represent an event or risk to be managed by both parties to minimise the risk to POL's business. The list is not intended to be exhaustive:

- Adverse weather
- Fuel strikes
- Criminal or terrorist activity directly affecting the ability to deliver service e.g. ram raids
- 3rd Party Service Provision
    - E.g. DVLA for on-line service
    - BT where telecom supply is outside POA or POL control

FUJ00079946

4.0 Trigger Topology

This document is covering the mutual responsibility between POL and POA for sharing information in the event of major incidents. POA however do not have responsibility for all aspects of the POL business domain. The following diagram illustrates the trigger topology.



FUJ00079946

FUJ00079946

Trigger Types

4.1.1 General

The full list of triggers is documented in CS/PLA/079. Other vulnerabilities are documented in SRRCs. The following paragraphs illustrate the types of trigger at a high level.

4.1.2 Branch trigger types

Branch major incident triggers are as follows:

- **Time of day** e.g. mornings 09:00 – 10:00
- **Time of week** e.g. Monday
- **Time of year** e.g. Christmas & Easter, End of month/quarter DVLA
- **Scale of outage** e.g. number of branches affected
- **Geographical dispersion** e.g. all branches in a town/city/county
- **Business initiatives** e.g. product launches

  Duration e.g. more than an hour•

4.1.3 Network trigger types

Network major incident triggers are as follows:

- Complete outage of Energis network
- Complete outage of BT network
- Complete outage of VSAT sites

4.1.4 Infrastructure Components trigger types

Infrastructure component major incident triggers are as follows:

- Total loss of environments providing individual on-line service capability
- Breach of access to data centres
- Breach of security
- Virus outbreak
- Loss of inter-campus links

FUJ00079946

4.1.5 Data Centre trigger types

Data centre major incident triggers are as follows:

- Network/LAN outage
- Loss of Wigan/Bootle data centre
- Breach of security

4.1.6 On-Line Services trigger types

On-Line services major incident triggers are as follows:

- On-line service unavailable within Data centre (not counter level)
- Number of Branches not able to provide on-line services – as defined by POL
- 3rd party provided service failure – Link, Fujitsu Group

4.1.7 Support Capability trigger types

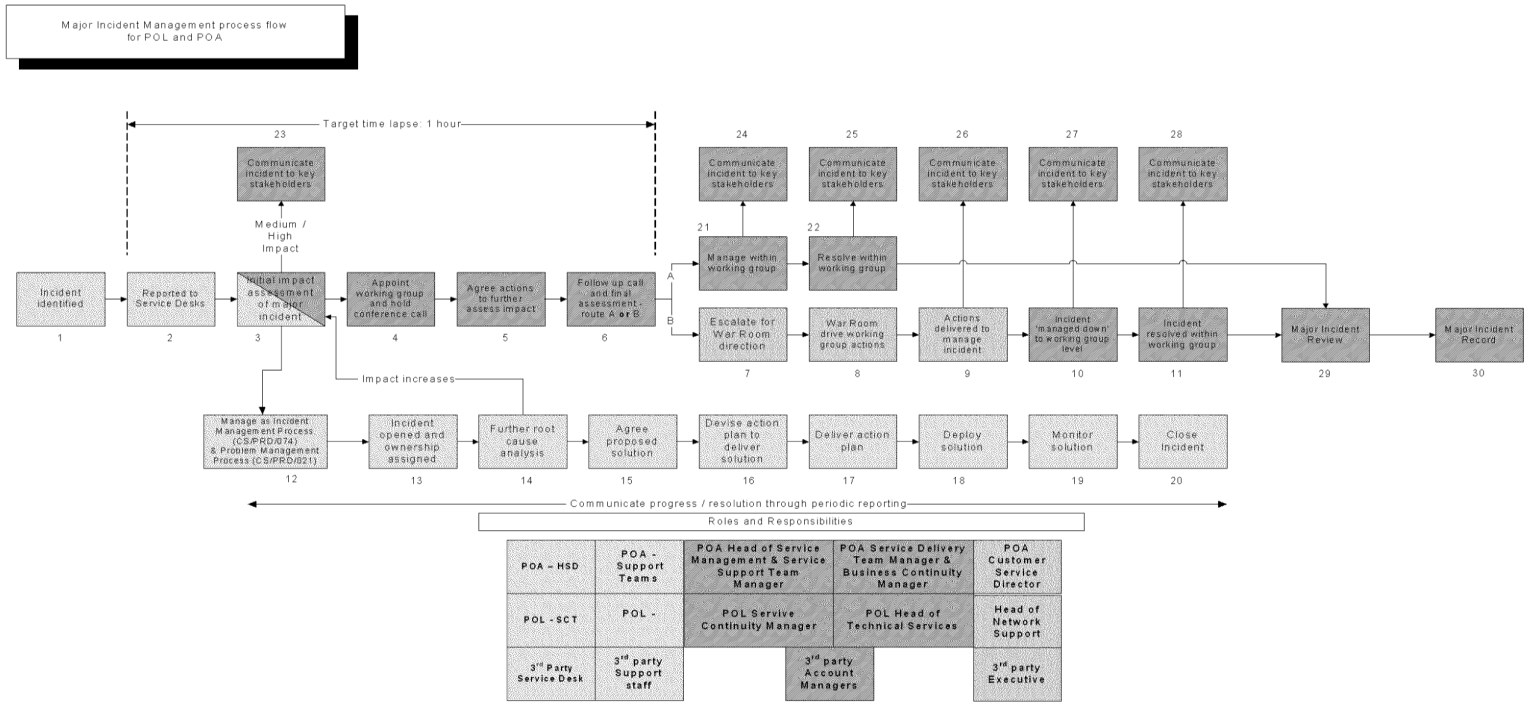
Support capability major incident trigger types are as follows:

- Fujitsu supplied infrastructure
  - Unable to raise OCP for "fix on fail"
  - Loss of E-mail
  - Unable to access Support Capability Systems
  - Access to support documentation
- Loss of Building providing support capability
  - Fire
  - Exclusion Zones
- Loss of key staff due to a major event
  - Terrorist attack

FUJ00079946

5.0 Process Flow

FUJ00079946



5.1 Process Description

FUJ00079946

Box	Title	Description	Key timescales	Action owner
1.	Incident identified	Incident identified, the definition of an Incident is "Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service." (CS/PRD/074). An Incident may be reported from within POL domain, a supplier domain or other route		
2.	Reported to Service Desks: Post Masters to HSD/SMC HSD to POL SCT SDU to HSD/SMC 3rd Parties to HSD to POL SCT 3rd Parties to POL SCT to HSD	The incident is reported into the HSD/SMC from within POL domain, a supplier domain or other route. The incident is profiled as a potential Major Incident as outlined within this document, including consideration of all influencing factors, time, geographical coverage, business impact, security, public perception, duration and relevant business initiatives coinciding at POL. The line of business POA Service Delivery Manager or Duty Manager (out of hours) will be alerted, and is empowered to make decisions. POL SCT will also be alerted, subject to POA SDM agreement.		
3.	Initial impact assessment of incident	With agreement from POA Service Delivery Manager, or Duty Manager out of hours, a SMS will be sent to POA and POL Management from HSD in core hours or SMC out of hours alerting to the potential existence of a Major Incident. This SMS will be sent **unless** expressly forbidden by the POA Service Delivery Manager or Duty Manager. For	T + 3 If the Incident is classified a Major Incident SMS communication	HSD/SMC/POA Service Delivery Manager/POA Service Delivery Team

FUJ00079946

		clarity, the default position is to send the SMS once discussion has taken place with the POA Service Delivery Manager or Duty Manager and POL SCT. The SMS message will read, "This message is to alert the potential existence of a Major Incident impacting the live estate. A further update will follow in 15 minutes" POL SCT will have been advised, by HSD/SMC. POL SCT will have contacted Richard Ashcroft immediately, who may contact the POA Service Delivery Manager or Duty Manager directly. The POA Service Delivery Manager will advise the POA Service Delivery Team Manager who will in turn advise: • Service Support Team Manager • Service Management Team Manager • Customer Service Director Upon initial confirmation of a Major Incident impacting the live estate, the POA Service Support Team Manager manages the incident from this point forward. An initial impact assessment of the incident is undertaken by members of the POA Service Team in consultation with POL, taking into account impact on: • Live Service	will be invoked within 3 minutes of classification. T + 15. All timescales quoted within this document as viewed as maximum, to be improved upon wherever possible.	Manager POA Service Support Team Manager

FUJ00079946

		• Financial Integrity • Business Image The need for a Technical Conference Call will be established as appropriate based upon the impact of the Incident. This will involve POA Service Team (as appropriate to the specific Incident), SMC, SSC, Core Services, Networks, and HSD as appropriate for each Incident. The outcome of the Technical Conference Call will be determination of the Incident being classified as Major (medium to high impact) or Business As Usual (low). An initial action plan will be defined. If the Incident is assessed as a Major Incident the POA Service Owner and POA Service Support Manager will move into a Technical Bridge Area on 6th floor at Bracknell. An impact analysis will be produced referencing: • Volume of calls received regarding the Incident • Calls from 3rd parties • Support Team Analysis • References from SRRC • References from KEL • Reference to Major Trigger Table		

FUJ00079946

		A further SMS will be sent, this will read "A Major Incident is confirmed, impacting the live estate, POA working group in attendance, further update in 30 minutes" If the outcome of the Technical Conference Call is that the Incident is determined Business As Usual (low) then an SMS communication will be sent stating that the Incident is not a Major Incident. From this point forward, with the exception of box 26, which is the responsibility of the Service Support Team Manager, SMS communication, timing and delivery requests, becomes the responsibility of the POA Service Delivery Manager. 30-minute updates should be the norm wherever possible.		
If the incident is low impact go to box 12. If the incident is medium to high impact proceed to box 4(Communication box 23):				
4.	Appoint working group and hold conference call	The POA Service Support Team Manager appoints a working group specific to each incident to participate in the management of the incident. The working group will be made up of POA Service Support Manager, Service Delivery Manager, Service Team Manager, Support Team, Business Continuity Manager, 3rd party Account Manager along with relevant POL business/technical managers as appropriate to each incident. Request to join the working group will be made by SMS via HSD in core hours or SMC out of hours.	T + 35.	POA Service Support Team Manager POL Service Manager

FUJ00079946

		Communication will be via a conference call to be convened and chaired by POA Service Support Manager, this may include 3rd party representatives subject to domain. The POL Service Manager with input and assistance from POA will chair POL domain incidents.		
5.	Agree actions to further assess impact	**Conference Call 1**: An action plan is formulated and agreed. Time of next conference call is agreed.	T + 45.	POA Service Support Team Manager POL Service Manager
6.	Follow up call and final assessment – route A **or** B	**Conference Call 2**: Following feedback on actions further assessment of the situation takes place. A decision is then taken on whether to manage the incident within the appointed working group [route A] or escalate for War Room direction [route B]. **Please note**: Depending on the severity of the incident the decision to escalate may have already taken place.	T + 60.	POA Service Support Team Manager POL Service Manager
If route A is chosen go to box 21. If route B is chosen proceed to box 7:				
7.	Escalate for War Room direction	If the appointed working group are unable to provide a timely resolution to the incident it is escalated for MAJOR INDICENT ESCALATION GROUP direction via the	Timescale dependant on impact and	POA Service Support Team Manager

FUJ00079946

		establishment of a War Room. The nature of the incident determines which POA Service Team members and POL Managers are involved in the War Room but it would include all or some of the following: • POL General Manager IT • POL Head of Technical Services • POA Service Support Manager (War Room Chairman) • POA CS Director • 3rd party Executives • Appointed working group representatives as appropriate The purpose of the War Room is to: • Provide appropriate direction on Incident resolution • Provide added impetus to restoration of service ASAP • Involve 3rd party Executives • Define communication intervals to Key Stakeholders • Provide focused Incident Management in line with the	nature of incident.	POL Service Manager

FUJ00079946

		• impact and severity of the Incident.		
8.	War Room drive working group actions	War Room provide the appropriate direction on the incident resolution priorities.	Timescale dependant on impact and nature of incident.	POA Service Support Team Manager. War Room.
9.	Actions delivered to manage incident within POA	Plan developed to resolve the incident with POL and other support teams as appropriate. Communication to box 26.	Timescale dependant on impact and nature of incident.	POA Service Support Team Manager. War Room.
10.	Incident 'managed down' to control of Working Group level	Action agreed using standard technical work procedures across the estate. Communication to box 27.	Timescale dependant on impact and nature of incident.	POA Service Support Team Manager
11.	Incident resolved within working group	Verify incident is now resolved and can be closed. Communication to box 28.	Timescale dependant on impact and nature of incident.	POA Service Team Support Manager
Low impact incident [continued from box 3]:				

FUJ00079946

12.	Manage as Incident Management Process (CS/PRD/074) and Problem Management Process (CS/PRD/021) by Service Desk and Support Teams	The Service Desk and Support Teams manage low impact incidents using existing Incident Management Process (CS/PRD/074) and Problem Management Process (CS/PRD/021).		
13.	Incident opened and ownership assigned	On notification of the Incident an Incident record would be opened by HSD, and should no KEL already exist, agreement reached on the appropriate team to be assigned the Incident for investigation.	T + 15.	HSD (IMT and Service Delivery Manager if appropriate)
14.	Further root cause analysis	Investigation into the Incident is undertaken and a specific cause identified. **Please note**: This may mean that the Incident is escalated to 'Major Incident' status. If this is the case return to box 3.	Timescale dependant on impact and nature of incident.	POA Support Teams
15.	Agree proposed solution	A solution to the problem is agreed. This may be solely within POA or within 3rd party domains, as appropriate. Follow known KEL's wherever possible. Closure criteria are clearly defined.	Timescale dependant on impact and nature of incident.	POA Support Teams

FUJ00079946

16.	Devise action plan to deliver solution	POA Support Team work together to develop a plan for Incident resolution. The action plan should include details of the specific solution including: • Resources • Timescale • Service Impact Assessment • Defined Communication Plan • Defined Regression Plan • Go/No-Go Decision • POA CS CP	Timescale dependant on impact and nature of incident.	POA Support Teams
17.	Deliver action plan	Action plan is presented to appropriate management for agreement. An OCP will be raised and managed as described in Change Process (PA/PRO/001)	Timescale dependant on impact and nature of incident.	POA Support Teams
18.	Deploy solution	Once approved, the solution is scheduled and implemented to agreed timescales, delivering the approved OCP/CP or in the case of a Software fix via Release Management. Regression testing and assurance is accepted at this point.	Timescale dependant on impact and nature of incident.	POA Support Teams

FUJ00079946

19.	Monitor solution	The solution is monitored to ensure successful implementation. Post implementation appropriate monitors with the capacity to monitor through Tivoli and System Logs will be in place.	Timescale dependant on impact and nature of incident.	POA Support Teams
20.	Close Incident	Incident is resolved and the Incident record closed.	Timescale dependant on impact and nature of incident.	HSD/POA Support Teams
Route B [boxes 21 and 22]				
21.	Manage within working group	If the incident does not require senior management direction the existing POA Service Management Team can manage it through to resolution. The POA SDM will initiate SMS messages updated every 30-minutes.	Timescale dependant on impact and nature of incident.	POA Service Delivery Manager HSD/SMC
22.	Resolve within working group	Verify incident is now resolved and can be closed. A Major Incident Review now takes place as box 29.	Timescale dependant on impact and nature of incident.	POA Service Delivery Manager
Communication [boxes 23 to 28]				
23.	Communicate incident to	Details of the major incident are sent via SMS to the Key	T + 20.	Service

FUJ00079946

	Key Stakeholders	Stakeholders in POL Ltd and POA. An SMS text alert message is sent to advise that a major incident has occurred and that further detail will be sent out.		Delivery Manager via HSD
24.	Communicate incident update to Key Stakeholders	An update on current situation/status of the incident is sent via SMS to the full range of POA SMS groups including POL.	Timescale dependant on impact and nature of incident.	POA Service Delivery Manager HSD/SMC
25.	Communicate incident update to Key Stakeholders	An update on current situation/status of the incident is sent via SMS to the full range of POA SMS groups including POL.	Timescale dependant on impact and nature of incident.	POA Service Delivery Manager HSD/SMC
26.	Communicate incident update to Key Stakeholders	An update on current situation/status of the incident is sent via SMS to the full range of POA SMS groups including POL.	Timescale dependant on impact and nature of incident.	POA Service Support Team Manager HSD/SMC
27.	Communicate incident update to Key Stakeholders	An update on current situation/status of the incident is sent via SMS to the full range of POA SMS groups including POL.	Timescale dependant on impact and nature of incident.	POA Service Delivery Manager HSD/SMC
28.	Communicate incident	An update on current situation/status of the incident is sent	Timescale	POA Service

FUJ00079946

	update to Key Stakeholders	via SMS to the full range of POA SMS groups including POL.	dependant on impact and nature of incident.	Delivery Manager HSD/SMC
29.	Major Incident Review	A review of the Incident including consideration of: • Lessons learnt • Incident definition • What went well • Timeline • Changes required to infrastructure • A review of the Major Incident Communication Process • Root Cause Analysis * if known at this point • Business impact • Action plan • Service Improvement Plan update	Within 24 hours of the Incident closure	POA Service Support Team Manager
30.	Major Incident Record	A written report detailing the agenda items of the Major Incident Review, for distribution to relevant POA, POL and 3rd party stakeholders.		POA Service Support Team Manager

FUJ00079946

6.0 Major Incident Escalation Procedures

6.1 Technical Conference Call

This is a technical conference for experts to discuss and analyse the incident enabling an appropriate action plan to be formulated to restore the service to POL without delay. The Technical Conference Call will baseline the anticipated response, covering resolution, time and resources required.

The Technical Conference Call will be incepted at T+15.

Telephone number for the Technical Conference Call is GRO, the Chairman will enter the call prior to the attendance of other callers and enter a designated PIN, allowing direct entry for subsequent callers.

Participants required on the call will be contacted via SMS as appropriate. The Service Support Manager will initiate the Technical Conference Call, with information passed onto the War Room if deemed appropriate.

6.2 War Room

The purpose of the War Room is to provide a focused area from which strategic decisions can be made regarding a Major Incident confirmed a MBCI.

Attendance will be mandatory from the following or their designated representative:

- POA Customer Services Director
- POA Service Management Team Manager
- POA Business Continuity Manager
- POA Service Delivery Manager (Business line specific)
- POL Head of Technical Services
- POL Service Continuity Manager
- POL Service Delivery Manager
- 3rd Party Account/Service Delivery Manager

Actions within the War Room include:

- Agreement of Containment Plan
- Documentation of all agreed actions with owners, and timescales
- Consistent management of the major incident across all involved locations
- Co-ordinate meeting times and locations

FUJ00079946

In the event of a major incident requiring a War Room to be incepted, it is envisaged that this will be in place at T+60. Participants required in the War Room will be contacted via SMS as appropriate.

Telephone number for the War Room working group is GRO the Chairman will enter the call prior to the attendance of other callers and enter a designated PIN, allowing direct entry for subsequent callers.

FUJ00079946

7.0 Roles and Responsibilities

This section defines the roles and responsibilities individuals and teams have with regard to the Major Incident Escalation Process.

Role	Responsibilities
HSD (IMT) Core Hours SMC Out of Hours (to IMT in Core Hours)	Log calls received from Post Masters and from the Post Office Service Continuity Desk Place and progress calls with support for investigation. Notify Post Office Account Service Delivery Manager (Duty Manager, out of hours) of incidents impacting /with potential to impact the live estate Escalate Central point of contact for progress updates and deployment of SMS messages.
POA Service Teams POA Technical Design Architectes POA Dev Managers	Respond to Incident or system faults. Diagnose and impact the incident. Attend Technical Bridge meetings & carry out service recovery tasks within the agreed action plan in order to recover the service to the customer. POA TDA's and Development Managers involvement will be dependant upon the level, severity and potential business impact of the Major Incident under review and will be via the Technical Conference Call.
POA Service Delivery Manager	**Service Delivery Managers and Duty Managers maintain the same level of empowerment as previously exercised. Responsibility, particularly out of hours, lies with the Duty Manager to decide incident resolution routes most suitable for the delivery of the highest level of customer service.** Initial impact assessment Management of team resources involved in the incident including the need for 3rd party involvement. Notify the POL Service Delivery Manager of initial findings and if inconclusive and requiring additional parties to be involved, instruct that a Technical Bridge be initiated. Inform POL of issues with regard to the live estate

FUJ00079946

	Communication Co-coordinator during a major incident Communication to POL Business Continuity Manager and POL Service Delivery Managers. Agreeing content of Communication updates. Appointment of a single problem owner to coordinate investigation.
Core Service Support Team Managers	Management of Core team resources involved in the incident Attend Technical Bridge meetings & carry out service recovery tasks within the agreed action plan in order to recover the service to the customer. Ensure that Core Services Senior Management is notified of the major incident and the impact presently in relation to the live estate within the organisation (Escalation Procedure IS/POA FJ/POA/NET/REF/076).
POA Service Support Team Manager Or Most Senior POA Manager present.	Appointment of a single problem owner to coordinate investigation. Initiates the technical bridge meeting if required subject to the severity of the incident and number of technical support teams required to resolve the incident. Calling all appropriate parties together in a 'War Room' at the outset to establish situation and develop action plans. Ensuring effective communication lines Ensuring Major Incident management is followed Ensuring War Room meetings include updates on actions agreed at start of each new session. Developing Communicating Action Plan Developing Containment Action plan. Developing Recovery Action Plan. Chairman of the Technical Bridge. Identifying Technical Expects required for investigation. Management /co-ordination of 3rd party Support Managers, escalation to 3rd party Account Managers and 3rd party 3rd/4th line technical experts, if required throughout the duration of the incident
POA Business Continuity Manager	Business Continuity Manager is the contact for coordinating Executive decisions and communication directives from Exec. Attending 'War Room' Major Incident meeting

FUJ00079946

	Ensuring representation in meeting to agree high-level action plans. Notifying the Post Office Business Continuity Manager on the status of the incident and appropriate action plan to be agreed and subsequently implemented.
POA Head of Service Management	Ensures appropriate Service Management resources are available to manage the incident and return the service to normal operation. Informs counterpart in Post Office of incident and progress Escalates to POA Customer Service Director
POA Customer Service Director	Liaises with POL IT Director and POL General Manager (Network Support Services) Escalates to POA Account Director if appropriate

FUJ00079946

8.0 Appendices

8.1 Escalation Communication Protocol

The primary principle:

Up"

and

"Across

Escalation protocol:

Fujitsu; Service Owners	SCT / Problem Managers
Service Delivery Team Manager	Service Continuity Manager
Head of Service Management	Supplier and Service Performance Manager
Customer Service Director	Head of Network Support / IT Director

FUJ00079946

8.2 Major Business Continuity Incidents (MBCI)

Sub-System Component	Location of Failure	Loss of Capacity	Loss of Resilience	Loss of Services	Core Hours Impact	Predicted Recovery Time	Non-Core Hours Impact
Data-centre failure	Bootle Data-centre	50% loss of infrastructure capacity	Generally total loss of resilience. Loss of EMC Data-duplication	1, NBS service whilst NPS is failed over. 2, APS Quantum emergency, TES-QA access and OBCS database whilst Database server failed over 3, Delay in Bootle outlets connecting into Wigan. 4, Loss of POLFS Production and Development services.	1, No NBS service whilst NPS is failed over. 2, No OBCS 'foreign encashment service until Database server is failed over. 3, No online services until 'Bootle' outlets connect into Wigan. 4, No POLFS production service until fail-over of the Wigan POLFS QA-TEST	1, NPS – 1 hour 2, OBCS service 60 to 90 minutes for fail-over. 3, Bootle outlets should connect to Wigan within 1 minute. 4, fail-over of the Wigan POLFS QA-TEST server to run the Production service takes approximately 48 hours. Note full fail-over of the supporting servers and services	1, No NBS service whilst NPS is failed over. Approximately 2 hours between 18.00 and 08.00 2, No OBCS service for 120 to 150 minutes. 3, Bootle outlets should connect to Wigan within 1 minute. 4, Fail-over of the Wigan QA-TEST server to run the POLFS Production service takes approximately 48 hours. 5, Potential delay to Ref Data drops.

FUJ00079946

						to Wigan, e.g., KMS, ACS, OCMS servers etc will take approximately five hours.	6, Potential delay to Harvesting. 7, Potential delay of AP Client file transfers.
Data-centre failure	Wigan Data-centre	50% loss of infrastructure capacity	Generally total loss of resilience Loss of EMC Data-duplication	1, Delay in Wigan outlets connecting into Bootle. Loss of the OMDB and Tivoli monitoring. Loss of the POLFS QA-TEST service	1, No online services until 'Wigan' outlets connect into Bootle. 2, The Tivoli master TMR, PO gateways and OMDB require fail-over to Bootle	1, Wigan outlets should connect to Bootle within 1 minute. 2, fail-over of the Tivoli infrastructure takes approximately 3 hours during core hours	1, Wigan outlets should connect to Bootle within 1 minute. 2, fail-over of the Tivoli infrastructure takes approximately 4 hours during non-core hours 3, Potential delays for the distribution of software via Tivoli.
Inter-Campus Link	Both Links	100% loss of Inter-Campus Link capacity	Total Loss of EMC Data-duplication	Both Data-centre operating in isolation. No cross campus data synchronisation.	1, Loss of NBS service to Wigan. 2, Maestro running on the Bootle Database server loses The ability to schedule work on any Wigan maestro agents.	Recommendation: 1,Manually perform a closedown of the Wigan LAR and ISDN routers to force all Wigan connected outlets to Bootle. This would take approximately 30 minutes. 2, Fail-over the	Recommendation: 1,Perform a closedown of the Wigan LAR and ISDN routers to force all Wigan connected outlets to Bootle. This would take approximately 90 minutes. 2, Fail-over the

FUJ00079946

						Tivoli infrastructure (Tivoli master TMR, PO gateways and OMDB) this takes approximately 3 hours during core hours	Tivoli infrastructure (Tivoli master TMR, PO gateways and OMDB) this takes approximately 4 hours during non-core hours. 3, Potential delays for the distribution of software via Tivoli.
Database Server	Bootle	No loss of Database server capacity	Total loss of Database server resilience	1, Loss of OBCS service whilst Database server manually failed over. 2, Loss of TES QA functionality while the server is manually failed over. 3, Loss of Quantum emergency file delivery to the counters until the server is manually failed over.	1, No OBCS 'foreign encashment service until Database server is failed over.	1, Database server fail-over to Wigan takes approximately one hour within core hours.	1, Database server fail-over to Wigan takes approximately two hours during non-core hours.
NPS (Dual Node)	Bootle	No loss of NPS capacity. (I.e. the NPS is only run from 1 data-centre at a time.)	Total loss of NPS resilience	Loss of NBS service whilst NPS manually failed over	1, No NBS service whilst NPS is failed over.	1, NPS fail-over takes approximately 1 hour during core hours.	1, NPS fail-over takes approximately 2 hour during non-core hours.

FUJ00079946

EMC Disc Array	EMC Disc Array at Bootle Data-centre	50% loss of EMC Array capacity	Total loss of EMC Data-duplication. Total impact on services running from Bootle	This equates to a loss of Bootle Data-centre (See entry above)	This equates to a loss of Bootle Data-centre (See entry above)	Recommendation: Consider performing a controlled fail-over of Bootle Data-centre services to Wigan. See loss of Bootle triggers above for impact to services.	Recommendation: Consider performing a controlled fail-over of Bootle Data-centre services to Wigan. See loss of Bootle triggers above for impact to services.
	EMC Disc Array at Wigan Data-centre	50% loss of EMC Array capacity	Total loss of EMC Data-duplication. Total impact on services running from Wigan	This equates to a loss of Wigan Data-centre (See entry above)	This equates to a loss of Wigan Data-centre (See entry above)	Recommendation: Consider performing a controlled fail-over of Wigan Data-centre services to Bootle. See loss of Wigan triggers above for impact to services.	Recommendation: Consider performing a controlled fail-over of Wigan Data-centre services to Bootle. See loss of Wigan triggers above for impact to services.
Catalyst Switch	Single Switch either Data-centre.	50% loss of internal campus LANs (resilience) and inter-campus link bandwidth	Total loss of internal campus LANs and Inter-Campus Link resilience	No loss of services. Wigan CAT 2 reduces the Master TMR and Tivoli monitoring capability	1, Very limited impact to on-line services (during fail-over.)	1, Automated fail-over very limited impact	1, Automated fail-over very limited impact
	Both Catalyst switches at Bootle Data-centre.	Total loss of internal campus LANs and total loss of inter-campus link bandwidth	Total loss of Bootle internal campus LANs and Inter-Campus Link resilience	This equates to a loss of Bootle Data-centre (See entry above)	This equates to a loss of Bootle Data-centre (See entry above)	Recommendation: Consider performing a controlled fail-over of Bootle Data-centre services to Wigan.	Recommendation: Consider performing a controlled fail-over of Bootle Data-centre services to Wigan.

FUJ00079946

						See loss of Bootle triggers above for impact to services.	See loss of Bootle triggers above for impact to services.
	Both Catalyst switches at Wigan Data-centre.	Total loss of internal campus LANs and total loss of inter-campus link bandwidth	Total loss of Wigan internal campus LANs and Inter-Campus Link resilience	This equates to a loss of Wigan Data-centre (See entry above)	This equates to a loss of Wigan Data-centre (See entry above)	Recommendation: Consider performing a controlled fail-over of Wigan Data-centre services to Bootle. See loss of Wigan triggers above for impact to services.	Recommendation: Consider performing a controlled fail-over of Wigan Data-centre services to Bootle. See loss of Wigan triggers above for impact to services.
Correspondence Servers	Loss of three Correspondence Servers in any cluster (Potential MBCI)	75% loss of Correspondence Server capacity for that cluster	Total loss of Correspondence Servers resilience in that cluster	Probable impact to online services connected in that cluster, depending upon transaction volumes.	Probable impact to online services connected in that cluster, depending upon transaction volumes.	NT SLA is 8 Hours. (Up to 8 Hours if all 3 failed simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if all 3 failed simultaneously).
	Loss of all four Correspondence Servers in any Cluster	Total loss of Correspondence Server capacity for that cluster	Total loss of Correspondence Servers resilience in that cluster	Total loss of online services at outlets connected to that cluster.	Total loss of online services at outlets connected to that cluster.	NT SLA is 8 Hours. (Up to 8 Hours if all 4 failed simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if all 4 failed simultaneously).
NBX Routing Agents	Loss of Bootle & Wigan Routing	Total loss of NBX routing capacity for the two clusters.	Total loss of NBX routing resilience for the two clusters	Total loss of NBS service for branches connecting to the two failed clusters, i.e.,	Total loss of NBS service for branches connecting to the two failed clusters, i.e.,	NT SLA is 8 Hours. (Up to 8 Hours if	NT SLA is 8 Hours. (Up to 8 Hours if

FUJ00079946

	Agents for two Clusters (1&3 or 2&4)			approximately 50% of outlets.	approximately 50% of outlets.	both Routing Agents fail simultaneously).	both Routing Agents fail simultaneously).
NBX Authorisation Agent	Loss of all Authorisation Agents for any FI (e.g. CAPO. LiNK, A&L)	Total loss of NBX capacity for that FI	Total loss of NBX resilience for that FI	Total loss of NBS service for the failed FI (e.g. CAPO. LiNK or A&L)	Total loss of NBS service for the failed FI (e.g. CAPO. LiNK or A&L)	NT SLA is 8 Hours. (Up to 8 Hours if the NBX Authorisation Agents fail simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if the NBX Authorisation Agents fail simultaneously).
NBX Data-centre LAN and/or Firewalls	Major fault affecting NBX internal LAN within either Wigan OR Bootle	50% loss of NBX capacity	Total loss of NBX resilience	Potential total loss of NBX service.	Loss of NBX service until LAN and NBX infrastructure in the data-centre with the fault is shutdown and the NBX services are manually stopped and switched to the operational data-centre.	Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to one data-centre. From time of determining that NBX service manual fail-over is required allow approximately 15 minutes.	Loss of NBX service until LAN and NBX infrastructure in the data-centre with the fault is shutdown. Unknown. Recovery time is dependant upon the fault conditions and diagnosis that failure is restricted to one data-centre.
NBX WAN Network to one or more FI.	Major fault affecting NBX external WAN from	50% loss of NBX bandwidth capacity to the FI(s)	Total loss of NBX WAN resilience to the FI(s)	Potential total loss of NBX service.	Loss of NBX service until external firewalls and NBX infrastructure in the data-centre with the fault is shutdown	Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to	Loss of NBX service until the WAN and NBX infrastructure in the data-centre with the fault is

FUJ00079946

	either Wigan OR Bootle				and the NBX services are manually stopped and switched to the data-centre from which the NBX WAN is operational	one data-centre. From time of determining that NBX service manual fail-over is required allow approximately 15 minutes.	shutdown. Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to the WAN or external firewalls in only one data-centre.
DCS/ETS Authorisation Agent	Loss of both DCS/ETS Authorisation Agents for a cluster	Total loss of DCS/ETS capacity for that cluster	Total loss of DCS/ETS resilience for that cluster	Total loss of DCS/ETS service for branches connected to the failed cluster.	Total loss of DCS and ETS service for one cluster, approximately 25% of Branches.	NT SLA is 8 Hours. (Up to 8 Hours if the DCS Authorisation Agents fail simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if the DCS Authorisation Agents fail simultaneously).
DCS/ETS Data-centre LAN and/or Firewalls	Major fault affecting DCS internal LAN within either Wigan OR Bootle	50% loss of DCS/ETS capacity	Total loss of DCS/ETS resilience	Potential total loss of DCS and ETS services.	Loss of DCS and ETS services until LAN and DCS infrastructure in the data-centre with the fault is shutdown and the DCS services are forced to switch to the operational data-centre.	Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to one data-centre. From time of determining that DCS services require fail-over to the alternative data-centre allow	Loss of DCS and ETS services until the LAN and DCS infrastructure in the data-centre with the fault is shutdown. Unknown. Recovery time is dependant upon the fault conditions and diagnosis that failure is restricted to one data-centre.

FUJ00079946

						approximately 15 minutes.	
DCS/ETS WAN Network to one or more FI.	Major fault affecting DCS and or ETS external WAN from either Wigan OR Bootle	50% loss of DCS and/or ETS bandwidth capacity to Streamline and/or E-Pay.	Total loss of DCS and/or ETS WAN resilience to Streamline and/or E-Pay.	Potential total loss of DCS and/or ETS service(s).	Loss of DCS service until external firewalls and DCS and/or ETS infrastructure in the data-centre with the fault is shutdown and the DCS/ETS services are manually stopped and forced to switch to the data-centre from which the DCS and/or ETS WAN is operational	Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to one data-centre. From time of determining that DCS/ETS service requires forcing to fail-over to the alternative data-centre allow approximately 15 minutes.	Loss of DCS and/or ETS service until the WAN and DCS and/or ETS infrastructure in the data-centre with the fault is shutdown. Unknown. Recovery time is dependant upon fault conditions and diagnosis that failure is restricted to the WAN or external firewalls in only one data-centre.
Energis 'Switch Exchange'	Loss of any Energis Point of Presence (E.g., Watford, Birmingham , Kersley) in a disaster.	Total loss of capacity to all outlets (ADSL) connected via that Energis site (e.g. multiple loss of BAS Routers)	Total loss of resilience.	Total loss of online services to all outlets (ADSL) connected via that Energis site (e.g. multiple loss of BAS Routers)	Loss of on-line services to all Branches on the unavailable BAS routers.	Reconfiguring Branch connections via BAS routers at alternative Energis Points of Presence takes approximately 24 hours.	Reconfiguring Branch connections via BAS routers at alternative Energis Points of Presence takes approximately 24 hours.
Post Office Limited –	Post Office Limited –	Total loss of capacity until	Total loss of resilience.	Major impact to:	No impact to Branch online services.	No impact to online services.	No impact to online services.

FUJ00079946

Northern Data-centre	Northern Data-centre	SunGard at Hounslow fully active		OpTIP, LFS, SAPADS, EDG, POL TES, POLFS.	LFS, SAPADS and POLFS services adversely affected.	Fail-over to the NDC DR site takes approximately 48 hours.	OpTIP, LFS, SAPADS, EDG, POL TES, POLFS services adversely affected. Fail-over to the NDC DR site takes approximately 48 hours.
POLFS (SAP) Production Service	POLFS Production Service at Bootle.	Total loss of capacity until POLFS QA-TEST service is activated as the DR Production service	Total loss of resilience.	Major impact to POL Financial Services.	No impact to online services at Branches.	Fail-over of the Wigan POLFS QA-TEST service to become the POLFS Production Service takes 48 Hours	Fail-over of the Wigan POLFS QA-TEST service to become the POLFS Production Service takes 48 Hours
DVLA Web Servers	Loss of both DVLA Web Servers, i.e., at both Data-centres	Total loss of DVLA capacity	Total loss of DVLA resilience	Total loss of DVLA online service for all Branches	Total loss of DVLA online service for all Branches	NT SLA is 8 Hours. (Up to 8 Hours if the DVLA Web Servers fail simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if the DVLA Web Servers fail simultaneously).
WAN Network Connection to DVLA	Major fault affecting DVLA external WAN from either Wigan OR	50% loss of bandwidth capacity to DVLA.	Total loss of AN Network resilience to DVLA	Potential total loss of DVLA service(s).	Total loss of online DVLA service until external firewalls and/or DVLA WAN infrastructure, for the specific data-centre with the fault, is	Unknown. Recovery time is dependant upon fault conditions and the diagnosis that failure is restricted to one data-centre.	Unknown. Recovery time is dependant upon fault conditions and diagnosis that the failure is restricted to the WAN or external

FUJ00079946

	Bootle				shutdown and the DVLA services are forced to switch to the data-centre from which the DVLA WAN is still operational	From the time of determining that DVLA service requires forcing to fail-over to the alternative data-centre allow approximately 15 minutes.	firewalls in only one data-centre.
PAF Web Servers	Loss of two PAF Web Servers, i.e., both servers at each Data-centre.	Total loss of PAF capacity	Total loss of PAF resilience	Total loss of PAF online service for all Branches	Total loss of PAF online service for all Branches	NT SLA is 8 Hours. (Up to 8 Hours if the PAF Web Servers fail simultaneously).	NT SLA is 8 Hours. (Up to 8 Hours if the PAF Web Servers fail simultaneously).
Data-centre Outlet Routers (ISDN, LNS, LAR)	Router failures at one data-centre, Wigan or Bootle	50% loss of Router capacity	Total loss of Router resilience	Total loss of online services for approximately 50% of Branches	Total loss of online services for approximately 50% of Branches. Shutdown any faulty Routers at the one data-centre to force Branches across to the alternative data-centre.	Allow 15 minutes for manual shutting down of Routers and forcing of Branches across to the alternative data-centre	Allow 75 minutes for manual shutting down of Routers and forcing of Branches across to the alternative data-centre Note software drops and Ref. Data drops could be affected during non-core hours.

FUJ00079946

Horizon Support Building (e.g., BRA01, STE09, IRE11)	Loss of primary site. E.g. BRA01, STE09, IRE11	Loss of approximately 66.66% capacity. (I.e. DR sites generally small that original office area.)	Total loss of resilience as each site has one primary Disaster Recovery location, e.g., FEL01, STE14 and Bridgeview.	None or limited impact to Services whilst DR to the alternative site is invoked.	Invoke DR and relocation to the alternative site.	STE14 and Bridgeview relocation approximately 30 minutes. BRA01 relocation to FEL01 approximately 2 hours for Hot standby equipment and approximately 1 week for cold standby equipment.	STE14 and Bridgeview relocation approximately 90 minutes, non-core hours. BRA01 relocation to FEL01 approximately 3 hours for Hot standby equipment and approximately 1 week for cold standby equipment.
People (e.g., SOS, SMC, SSC, POA SI, POA CS)	Any Team	Dependant upon the nature of a disaster	Dependant upon the nature of a disaster	Potential impact to both online and offline services.	Consider reallocation of resources across teams as appropriate.	Probably >48 hours.	Consider reallocation of resources across teams as appropriate.

FUJ00079946