FUJ00001981

_

Document Title: **HORIZON SERVICE DESK BUSINESS CONTINUITY PLAN**

Document Type: **CONTINGENCY PLAN**

Release: Not Applicable

Abstract: This plan provides a summarised description of the Horizon Service Desk (HSD) which supports the Horizon service. The document also details the planned actions that will be taken to minimise the risk of this service not being available.

Document Status: **APPROVED**

Originator & Dept: Tony Wicks, POA CS Business Continuity.

Contributors: Nigel Bailey, FSCS Business Continuity.
Various HSD staff.

Internal Distribution: POA Management Board, D Baldwin, C Marx, R Brunskill, M Stewart, T Wicks, M Woolgar, I Daniel, J Welsh, N Bailey (FSCS), P Gardner (FSCS), M Croucher (FSCS)

External Distribution: Adam Martin, Post Office Limited Business Continuity Planning Manager

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

Name	Position	Signature	Date
Dave Baldwin	Director, POA Customer Service		
Adam Martin	Post Office Ltd. Service Continuity Manager		

FUJ00001981

0.0 Document Control

0.1 Document History

Ver No.	Date	Reason for Issue	Associated CP/Peak
0.1	12/03/99	Initial draft	None
0.2	14/05/99	This document now incorporates significant internal and external comments.	None
1.0	30/06/99	All non-relevant references to the DSS removed.	None
1.1	08/11/99	Minor changes made to associated document references and update to contact details. Issued for formal review.	None
1.2	16/12/99	Changes following review by POL and internal Pathway review.	None
2.0	28/01/00	Changes following review and comments from POL - 26th January 2000. Issued for Approval	None
2.1	18/05/00	Creation of section 4.2.3 and amendments to sections 0.3, 4.2.2 and 12.	None
2.2	11/08/00	Amended to incorporate comments from Dave Hulbert, POL and Paul Westfield, Pathway.	None
3.0	06/09/00	Amended for comments raised by Dave Hulbert (POL) in comment sheet QR905.	None
3.1	09/05/01	Updated by N Bailey (FSCS) following review by HSD	None
3.2	16/05/01	Updated by N Bailey (FSCS) following review by Tony Wicks	None
3.3	11/07/01	Various changes by Tony Wicks to reflect the introduction of WAK01 HSD site, changes to the voice systems and ACD.	None
3.4	11/09/01	Updated by Tony Wicks to reflect the introduction of Single Point of Contact and for the formal cross-domain comment cycle.	None
3.5	10/12/01	Updated by Nigel Bailey after review by HSD December 2001	None
3.6	11/01/02	Incorporates comments from Stephen Potter (Post Office Limited) and Tony Wicks. Pathway Requirements Approval Authority withdrawn.	None
4.0	07/02/02	Issued for formal approval.	None
4.1	20/11/02	Updated by Nigel Bailey after review by HSD Nov 2002, prior to Network Banking release and Technical Service Desk introduction.	None
4.2	03/12/02	Incorporates comments from Tony Wicks	None
4.3	04/12/02	Updated by N Bailey FSCS following review by Tony Wicks	None
4.4	09/12/02	Incorporates comments from Peter Burden and Philippa Whittington	None
5.0	30/01/03	Incorporates comments from Dave Hulbert, Philippa Whittington and Peter Burden.	None
5.1	14/03/03	Updated by N Bailey for HSD and HIT being single site	None
5.2	21/03/03	Updated by N Bailey after review by HSD	None
5.3	02/04/03	Minor updates by Tony Wicks before formal review cycle.	None

FUJ00001981

_

6.0	07/05/03	Comments from formal internal review.	None
6.1	19/02/04	Updates by N Bailey after review with HSD.	None
6.2	23/02/04	Updates by N Bailey following a review by HSD. Further updates applied by Tony Wicks prior to review cycle.	None
6.3	22/04/04	Section 4.1.1 revised for comments from Philippa Whittington. Formally issued for approval	None
6.4	12/11/04	Revised by Mark Shaw and Tony Wicks after the Technical Support Desk was withdrawn	None
6.5	03/12/04	Amended for comments received from the review cycle.	None
7.0	06/12/04	Formally issued for approval.	None
7.1	14/12/05	Updated by N Bailey: Doc name Change / HSH to HSD / contact details / risk updates / SMC DR changes / Add IMT / Ref doc updates	None
7.2	19/12/05	Minor updates by Tony Wicks prior to circulating for formal review	None
7.3	12/01/06	Incorporated comments for Tim Vause Post office Limited, Paul Gardner and Richard Brunskill.	None
8.0	30/01/06	Formally issued for approval. (Version 7.3 was distributed to the mandatory reviewers by the author prior to creating version 8.0)	None

0.2 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks

Mandatory Review Authority	Name
Post Office Limited Service Continuity Manager	Adam Martin (TV*)
Director POA Customer Service	Dave Baldwin
CS Head of Service Management	Carl Marx
CS Senior Service Delivery Manager	Richard Brunskill*
HSD Operations Manager (STE09)	Paul Gardner*
SMC Operations Manager	Ian Cooley
Optional Review / Issued for Information	
CS Service Delivery Manager (HSD)	Julie Welsh
Core Services Business Continuity Manager	Nigel Bailey

(*) = Reviewers that returned comments

FUJ00001981

0.3 Associated Documents

	Reference	Vers	Date	Title	Source
REF1	CS/SIP/002			Business Continuity Framework	PVCS
REF2	CS/PLA/079			Horizon Services Business Continuity Plan	PVCS
REF3	CS/PLA/080			Horizon Support Services Business Continuity Plan	PVCS
REF4	CS/PLA/011			Business Continuity Test Plan	PVCS
REF5	FRM/HSD/001			HSD BCP Notification and Escalation Process	
REF6	CS/PRD/021			Fujitsu Services (POA) Incident Management Process	PVCS
REF7	CS/PRD/031			Fujitsu Services (POA) CS Business Continuity Management	PVCS
REF8	SU/MAN018			Operations Procedures Manual Index	PVCS
REF9	PRO/HSD/001			Voice System Contingency Operating Procedure	FSCS - HSD
REF10	PRO/HSD/003			HSD Process For Utilising Contingency	FSCS - HSD
REF11	CON/MGM/005			Post Office Limited and Fujitsu Services Business Continuity Interface (OLA) Agreement	POL
REF12	PA/TEM/001			Fujitsu Services Document Template	PVCS
REF13	SMC\PRO\021			SMC Contingency	FSCS - HSD

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

0.4 Abbreviations/Definitions

Abbreviation	Definition
ACD	Automatic Call Distribution
BCM	Business Continuity Manager
BT	British Telecomm
DCS	Debit Card System
DR	Disaster Recovery
FSCS	Fujitsu Services Core Services Division
HSD	Horizon Service Desk (old name of the HSD)
HSD	Horizon Service Desk
IMT	Incident Management Team (Part of HSD)
MBCI	Major Business Continuity Incident
MIS	Management Information Service

FUJ00001981

–

NBX	Network Banking Service (the NBS Replacement service)
OBCS	Order Book Control Service
OOH	Out Of Hours
OSP	One Shot Password
POA	Post Office Account
PM	Post Master
POL	Post Office Limited (previously Post Office Networks)
SDC01	Southern Data Centre
SLT	Service Level Target
SMC	Systems Management Centre
SOS	Systems Operate Service
SSC	System Support Centre
STE09	HSD primary site in Stevenage
STE14	HSD disaster recovery site in Stevenage
UKME	UK Mobile Engineering

0.5 Changes in this Version

Version	Changes
7.0	Issued for formal approval.
7.1	Updated by N Bailey: Document name changed from HSH to HSD, contact details updated, risk table updates, SMC DR changes, incorporated the IMT and document Ref section updated.
7.2	General updates by Tony Wicks, including revising escalation and contact details and an explanation of the IMT function.
7.3	Amended HSD Ops Manager contact details in section 12.0. Removed SVR (Service Visit Reply) from section 4.1.1 and revised Post Office Limited contact details in section 12.0 Replaced all references of 'PowerHelp' to 'Phoenix' in preparation for the integration of the Phoenix/web service. Updated section 4.2.2 IT Systems to include references to the new Phoenix Application and Web servers
8.0	Issued for formal approval.

0.6 Changes Expected

Changes
This is an operational document, which will be amended for numerous reasons including: 1, new risks are identified; 2, improved or new contingency actions are identified; 3, there are operational changes to the HSD services or infrastructure;

FUJ00001981

–

4, changes to bring this plan inline with the new contract.

FUJ00001981

0.7 Table of Contents

FUJ00001981

_

1.0 Introduction

This Contingency Plan provides a summarised description of the Horizon Service Desk (HSD) and then goes on to document the measures taken to minimise the risk of not being able to provide this service.

The document then sets out what actions the Problem, Service or Business Continuity Manager will need to take to instigate any recovery or contingency procedures specific to the provision of this service.

2.0 Scope

This plan covers the following key areas.

- A summary of the service to which it relates
- A summary of the testing activities undertaken to validate the HSD Service solution
- 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 recovery can be referenced from the FSCS Operational Procedures Manual Index (REF8).

FUJ00001981

_

3.0 OWNERSHIP AND OPERATION

The Fujitsu Services POA Service Managers, own this plan and are responsible for its maintenance and operational verification. The FSCS Stream Manager operates this plan. Contact details are shown below.

Name	Position	Office Contact No.	Out of hours No.
Richard Brunskill	Fujitsu Services POA Senior Service Delivery Manager	GRO	GRO
Tony Wicks	Fujitsu Services POA Business Continuity Manager.	GRO	GRO
Martin Croucher	Fujitsu Services Stream Manager	GRO	GRO

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

FUJ00001981

_

4.0 FUJITSU SERVICES HELPDESK SERVICES FOR THE POST OFFICE

4.1 Introduction

The services provided by Fujitsu Services changed during the autumn of 2002 with the introduction of SPOC2 and Universal Banking.

A Single Point of Contact for all telephone calls from Post Masters, about Post Offices services, including the POA solution, is fully operational. Telephone calls are now taken via the NBSC Single Point of Contact with a voice driven menu system where callers are directed to choose the option for the Horizon Service Desk for specific issues.

This plan covers the following team providing technical services:

- Horizon Service Desk

HSD is operational Monday to Saturday from 08:00 to 18:30.

Notes:

An Incident Management Team also resides within the Horizon Service Desk function.

Please refer to the Systems Management section of the Horizon Support Service Continuity Plan (REF3) for details on the reporting of Out Of Hours incidents, e.g. for operational issues at Post Office Limited or AP client sites.

Much of the infrastructure, e.g. Phoenix, is common to the HSD, UKME 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 STE09 or SDC01.

4.1.1 Horizon Service Desk (HSD)

All calls are taken in STE09. The HSD service is provided out of normal HSD hours only by the use of a voicemail service.

The HSD provides the following services:

- Support for the following callers:
    - Authorised Post Office (Outlet) Staff
    - Authorised Post Office Limited Staff
    - All other authorised users as stated in the Call Enquiry Matrix DSP/HQ/OPS/001
- Incident logging and all diagnosis for callers entitled to use the Horizon Service Desk

FUJ00001981

- Call resolution or routing in line with contractual measures.
- Central point for information on the working state of the overall infrastructure (calls may be passed to the SMC depending on the information required).
- Responsibility for the overall management of the call from inception to resolution with regard to ensuring overall call progression is in line with contractual SLT's.
- Escalation of incidents where they are likely to breach their individual SLT or constitute a possible or actual business risk.
- Responsibility for analysing and escalating received incidents and for providing information on SLT conformance, incident trends and call-handling timescales.

The Incident Management Team is a team within the HSD who deal primarily with SLA monitoring, Trend Analysis, Escalations process, Major Incidents, Customer Complaints, Daily Hardware and network call-backs.

The IMT is broken down into two areas; those who deal solely with the daily hardware and network call back reports and those that deal with all other aspects of the role.

HSD uses the secure POA network to gain access to the TIVOLI management system which is in STE09.

4.2 Common Infrastructure

4.2.1 Voice Systems Features

With the introduction of the Single Point of Contact all calls into the Horizon Service Desk are routed via a single number operated by BT. This service has been stated to provide 100% resilience for call delivery into the HSD, and therefore Fujitsu Services has not provided any additional resilience in order to operate using this service. The invocation process for changing operational call plans has been modified to reflect the source of call delivery (being via Post Office Limited during normal operational hours and via BT at other times).

The HSD is located at a single site in Stevenage (STE09).

The STE09 HSD site has a target ISDN30 bearer receiving Post Office Limited calls via BT Command Link. The STE09 bearer is supported by two ISDN30 bearers, one of which has 15 live and 15 spare channels. Calls are automatically cascaded to the supporting bearers when the target bearer is busy.

In the event that the HSD site in STE09 is rendered inoperable (e.g. building evacuation), then calls can be either re-directed to a voicemail service, or redistributed to the HSD disaster recovery site in STE14, using BT remote divert and Command Link. If this cannot be handled automatically by the Network ACD or BT re-routing, then the 'remote divert' will be used to manually re-route calls within the BT network.

FUJ00001981

All calls diverted to the HSD disaster recovery site are directed to a direct dial number on the STE14 Private Automatic Branch Exchange (PABX).

Remote diverts can be activated, by approved managers, via the Post Office Limited NBSC. This may need to be used in conjunction with the temporary transference of reinforcement staff from the inoperable centre to a DR site.

4.2.2 IT Systems

A Phoenix database server, one Phoenix application server and one Phoenix Web server are all located at the STE09 HSD location. Standby Phoenix database, application and Web servers are also located in the Southern Data Centre in SDC01. The preferred working model is to run all three Phoenix Servers 'local' from the same site in order gain optimal performance from the system. However, an additional level of contingency has been introduced for such scenarios as hardware failures at both sites. E.g. A failure of the STE09 application server coupled with and a failure of the SDC01 web server could now potentially result in a continued service, e.g., by running the web server from STE09 and the application server from SDC01.

4.2.3 Power

To provide contingency against mains power failure, the HSD Phoenix Database servers, Application servers and Web servers, and the HSD telephone communications equipment in STE09 and SDC01 are protected by Un-interruptible Power Supplies. A standby generator is in place in STE09 and there are standby generators for the SDC01 Data centre. 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.

5.0 Testing Strategy

5.1 Initial Testing

The initial testing of all business continuity contingency plans is documented in the Business Continuity Test Plan (REF4). For details of the test objectives for the Horizon Service Desk and services and for an overview of the test, see test 10 in this reference.

5.2 Ongoing Test Strategy

This refers to how the contingency measures in place for the Horizon Service Desk (HSD) services will be periodically tested to ensure they are current and reflect the service model as the services matures.

This will be 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 reflected in the Business Continuity Test Plan (REF4).

FUJ00001981

6.0 Preventative Measures

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

This concept is extended to the provision of the Horizon Service Desk , thus allowing the helpdesk service to be delivered in part, or indeed in total, from one or more helpdesk sites (including Disaster Recovery sites) should the need arise.

7.0 Preparedness Measures

Preparedness in the Horizon 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 Service Management & Delivery

From a business perspective, this process starts by establishing very exacting and specific service level agreements with all suppliers to the Horizon 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 not only service level requirements but also the quality model.

7.2 Risk Analysis

Section 10 contains a risk analysis of the Horizon Service Desk service provision. This is supported by a more detailed risk analysis managed by the FSCS Horizon Service Desk.

This identifies potential risks to the 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 the service.

FUJ00001981

8.0 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 Horizon solution includes a Systems Management capability to monitor and report on events that occur upon the infrastructure platforms involved in the Horizon service delivery.

Most events that could lead to a break in the HSD service will be recognised by, operational staff detecting a loss of infrastructure (such as power, phones etc), or through observation by one of the support groups using system monitoring equipment.

In addition major hardware components (network links and servers) are remotely monitored and faults can be reported by the monitoring services.

8.2 Activation

Once an event has occurred that will impact the provision of the HSD, a service call will be raised with the most appropriate support unit via a call to the internal Fujitsu Services helpdesk service (7799), or direct to the support unit.

8.3 Incident Management

In the event of a major incident the HSD Duty Manager will take command and follow HSD procedures (REF10) to implement appropriate actions.

If the incident cannot be resolved by the HSD 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 HSD escalation criteria, it will be escalated to the appropriate Fujitsu Services POA CS Service Delivery Manager or Duty Manager. The POA CS Service Delivery Manager or Duty Manager will use the POA Incident Management Process (REF6) to decide if a problem exists.

If the criteria for Cross-Domain Business Continuity Management are satisfied the POA Duty Manager will escalate the incident to the Fujitsu Services POA Business Continuity Manager as a Business Continuity incident.

Note: Post Office Limited may also escalate Business Continuity incidents directly to the POA Duty Manager.

8.4 Initiation of recovery procedures

Where this is a POA only problem, recovery would usually be instigated by the support team charged with supporting the equipment upon which the failure has occurred, as

FUJ00001981

soon as possible, and certainly with intent to resolve the problem within the relevant Service Level Target.

Depending on the severity of the problem, there may be some dialogue between the POA Duty/Problem Manager and the support function to agree on the most appropriate course of action.

Where there is a Cross-Domain problem, 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 11 Plan Activation.

9.0 Recovery of Normal Service

All aspects of the HSD service infrastructure within POA are managed operationally by FSCS. As such, the process of recovering from an event causing an impact to the service will by definition involve FSCS, and or other support services within Fujitsu Services, in performing an operational activity to resume the full service.

FSCS have prepared operational procedures that are referenced from the index (REF8). The procedures either document the recovery activities from all possible failures in the end to end service or reference related operational documents used by Fujitsu Services.

For simple problems, normal service could be resumed without the need to notify the POA CS Service Delivery Manager or Duty Manager, for more involved problems the Duty or Problem Manager would liase with the support teams, agreeing when the recovery action should be run, and then carrying out that activity.

FUJ00001981

10.0 Impact & Risk Assessment

The table below summarises the identified risks to the provision of the HSD services.

As a matter of normal operational practice, a call would be placed against HSD (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 HSD.

The table within section 10.1 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.

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 complete 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, FSCS HSD Service Management and the Fujitsu Services POA project team have developed a vast knowledge of component failure and service availability over the life of the service.

FUJ00001981

10.1 Risks Identified Against Horizon Service Desk / Incident Management Team

No	Service Element	Risk	Probability	Critical Time Factor	Impact	Action
1.	BT telephone call delivery system via SPoC IVR system	Any failure by BT lines into SpoC (at POL)	1	Immediate	Total loss of HSD service Possible SLT Failure **Possible Business Impact:** **POL, POA, HSD**	(100% service requirement placed on BT via resilient systems, links contracted to POL not POA, therefore no contingency possible within POA) Log test calls / investigate Resolve via HSD incident process Consider site relocation for some staff to the DR site. **MBCI Go to 10.2.1** **Inform: POL BCT**
2.	MITEL ACD telephone system – STE09	For any reason.	2	Immediate > 60 mins	**Minimal Impact:** Major Call queuing Probable SLT failure **Potential Business Impact on HSD and POA**	**For HSD:** See section 4.2 UPS would provide emergency power for up to 4 hours, then a generator would provide power. Invoke BT Command Link to switch to voicemail & put message on IVR via NBSC

FUJ00001981

						Resolve via HSD incident process > 60 mins consider temp site relocation to DR site **MBCI Go to 10.2.2** **Inform: POL BCT**
3.	Loss of access to TIVOLI at STE09 HSD	Any failure Total Loss	2	< 120mins > 120mins	**Minimal impact**: HSD - No ability to handle calls that require ability to access a PO Counter system Probable SLT failure **Business Impact:** **HSD, POA, POL**	Resolve via incident management process. Request MSS & SMC to assist. **Potential MBCI Go to 10.2.5** **Inform: POL BCT**
4.	Voicemail failure for OOH calls	Any failure	0	> 4 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**
5.	STE09 HSD non-operational	For any reason HSD lost of 100% capacity	1	< 30mins > 30mins	**Minimal impact** **Major Impact.** Call queuing No calls being taken by HSD Probable SLT failure if over an extended period.	**For HSD:** Invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and POA Data Centres.

FUJ00001981

					Business Impact: **HSD, POA and POL**	Consider relocation to DR site in STE14 for HSD and BRA01 for selected IMT staff. Resolve via HSD incident process. **MBCI Go to 10.2.2** **Inform: POL BCT**
6.	Loss of people in STE09 - HSD / IMT	Loss of access to most staff	0	< 30mins > 30mins	**Minimal impact** **Major Impact.** No calls being taken by HSD Call queuing Probable SLT failures **Business Impact:** **HSD, POA and POL**	**HSD** must invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and POA Data Centres. Consider relocation to DR site in STE14 for HSD, and BRA01 for selected IMT staff Resolve via HSD incident process. **MBCI Go to 10.2.3** **Inform: POL BCT**
7.	Primary Phoenix System I.e., Web, Application or Database server	Any failure	2	< 30mins > 4hrs	**No impact** Unable to log new calls using Phoenix or access existing calls Possible call queuing whilst server is switched and running on manual logging. Loss of resilience whilst	Invoke manual logging. Perform switch over to secondary Phoenix servers. Add manually logged calls on secondary Database server. Use Enqweb archive or Phoenix archive to access existing calls Resolve via HSD incident

FUJ00001981

					restoration to normal service is being performed. **Minimal Business Impact: HSD**	management process.
8.	Secondary Phoenix server. I.e., Web, Application or Database server	Any failure Loss of resilience	1	> 24 hrs	Loss of resilience only **No Impact.**	Resolve problem via HSD incident management process.
9.	Failure both Phoenix primary and secondary servers. I.e., any type, Web, Application or Database servers.	Any failure	0	Immediate > 8 hrs	Unable to log calls quickly. Possible queuing if calls levels high. Possible SLT failure if over an extended period. **Potential Business Impact: HSD, POA 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 workstation in STE09	Any circumstance All OSP workstations unavailable Lost 100% capacity	0	> 30 mins	Unable to resolve outlet problems **Business Impact: Minimal**	Resolve via incident management process Six One Shot Password workstation available for contingency Also DR One Shot Password workstation in STE14
11.	Phoenix to D1	Any failure	3	> 4 hrs	Automated process lost	Resolve problem via HSD incident

FUJ00001981

	OTI Link				**Minimal Business Impact:** **HSD / UKME** (Unless over an extended period with high call volumes)	management process. Fax details of calls that would be passed into D1 to UKME helpdesk
12.	Phoenix to Peak Link	Any failure	3	>30 mins	Automated process lost **Minimal Business Impact:** **HSD POA 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 (Wigan & Bootle)	0	> 30 mins	No access to Tivoli (see Risk 3) **Business Impact:** **HSD, POA, 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**
14.	Network links to Cable & Wireless for Phoenix	Any failure	1	> 4 hrs	Electronic access to Cable & Wireless helpdesk not available. **Business Impact: POA**	Resolve via incident management process. Fallback to manual processes.
15.	Loss of Corporate Network in STE09	For any reason	1	Immediate	HSD unable to access Phoenix and other services. This will slow call resolution. Unable to fully verify caller details. Loss of e-mail.	Network access to Phoenix is now localised and does not rely on fully functioning corporate network. If the Primary server is in SDC01 a switch to STE09 can be made.

FUJ00001981

					Loss of Log shipping causing loss of resilience. Possible SLT failures for HSD **Business Impact:** **HSD, POA, POL**	Invoke Manual call logging process. Resolve via problem management process. Consider relocation to DR sites if DR sites are unaffected **Potential MBCI Go to 10.2.4** **Inform: POL BCT**

FUJ00001981

10.2 Summary of Contingency Actions

10.2.1 BT Telephone Call Delivery System, via IVR (NBSC), to HSD.

There is no contingency action to be performed by HSD over and above normal operational incident processes and the actions identified within the above risk tables. This is a BT supplied service.

10.2.2 Loss of Functionality in STE09 for HSD

If STE09 is unavailable for use by HSD provision has been made for staff to re-locate to facilities in STE14, another Fujitsu Services site in Stevenage. 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 no HSD is available 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. Selected staff would relocate to BRA01 to access Tivoli based functionality.

10.2.3 People

Human Resource Management processes are in place to manage the normal turnover of staff.

10.2.4 Manual Processes due to total loss of Phoenix

In the event that the Phoenix servers have failed at both STE09 and SDC01, or are inaccessible, manual processes will be used to log calls until such time as Phoenix can be returned to service.

10.2.5 Loss Of access to Tivoli

In the event of the unavailability of Tivoli at STE09 for an extended period of time (at least 2 hours) then temporary relocation to BRA01 shall be considered.

FUJ00001981

11.0 Plan Activation

Once the criteria for Business Continuity involvement has been satisfied, i.e. an MBCI Trigger from the table of risks above (section10), and after a call has been placed, and appropriate details logged with the HSD (where possible), the problem ownership is passed to the POA member of the Business Continuity Management team.

After compiling all relevant information, and if necessary communicating this to the other members of the BCMT listed below (section 12), a full impact assessment will be conducted to determine if the Fujitsu Services POA Business Continuity Management Process (REF7) 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 step will be to agree whom 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. The planning 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 impacting the affected service has been resolved, and the MBCI closed.

Refer to REF18 for full details of the Fujitsu Services POA Business Continuity Management Process.

FUJ00001981

12.0 Contact List

12.1 Normal Processes

Organisation	Contacts	Telephone Number
Fujitsu Services POA	Duty Manager	Pager: GRO
	CS Head of Service Management	Office: GRO
		Mobile:
	CS Senior Service Delivery Manager	Office:
		Mobile: GRO
(MBCI Contacts)	Business Continuity Manager	Office: GRO
		Mobile: GRO
	CS Senior Service Delivery Manager	Office:
		Mobile: GRO
FS Core Services SOS Networks	Network Manager	Office:
		Mobile: GRO
	Network Management Centre Manager	Office:
		Mobile: GRO
FS Core Services SOS NT and UNIX	SOS NT and UNIX Manager	Office:
		Mobile: GRO
	Technical Support Manager	Office:
		Mobile: GRO
FS Core Services SMC	SMC Desk	Office: GRO
	SMC Duty Manager	Mobile: GRO
	MSS / SMG Business Manager	Office: GRO
		Mobile:
	SMC Operations Manager	Office:
		Mobile: GRO
	Business Stream Manager	Office:
		Mobile: GRO
FS Core Services HSD	HSD	HSD GRO
		Mobile: GRO
	HSD STE09 Duty Manager	
	HSD Operations Manager	Office: GRO
		Mobile:
	Business Stream Manager	Office: GRO
		Mobile:
Post Office Limited	Buiness Continuity Manager	Office: GRO
		Mobile:
	Service Continuity Manager	Office: GRO
		Mobile:

FUJ00001981

12.2 Escalation Processes

Escalation Level	Level 1	Level 2	Level 3	Level 4
Fujitsu Services POA	CS Senior Service Delivery Manager Office: GRO Mobile: GRO Duty Manager Pager: GRO	Problem Manager (Assigned by Duty Manager) BCM Office: GRO Mobile: GRO	Head of Service Management Office: Mobile: GRO	Customer Service Director Office: GRO Mobile: GRO
FS Core Services Networks			Network Manager Office: GRO Mobile: GRO	NMC Manager : Office: GRO Mobile: GRO
SOS NT and UNIX			NT& UNIX Manager Office: GRO Mobile: GRO	Technical Support Manager Office: GRO Mobile: GRO
SMC			SMC Manager Office: GRO Mobile: GRO	Bus Stream Mgr Office: GRO Mobile: GRO
HSD	HSD Duty Manager STE09 Duty Mobile: GRO	As per Level 1	HSD STE09 Ops Mgr Office: GRO Mobile: GRO	Bus Stream Mgr Office: GRO Mobile: GRO
Post Office Limited	Business Continuity Manager GRO Mobile GRO GRO	Business Continuity Manager GRO Mobile GRO GRO	Service Continuity Manager Office: GRO Mobile: GRO	Network Support Service Manager Office: GRO Mobile: GRO