_

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, RMGA CS Business Continuity.

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

Internal Distribution: RMGA Management Board, W Warham, S Denham, M Stewart, T Wicks, M Woolgar, K Gallacher, N Bailey (FSCS), G Stewart (FSCS), I Cooley (FSCS), R Batty (FSCS), M Jacklin (FSCS)

External Distribution: Gary Blackburn, Post Office Limited Business Continuity Manager

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

Name	Position	Signature	Date
Wendy Warham	Director, RMGA Customer Service		
Gary Blackburn	Post Office Ltd. Business Continuity Manager		

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, 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
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
8.1	29/03/06	Reinstated references to Powerhelp, i.e., removing the references to Phoenix which were incorporated in version 7.3 of this plan, as it was decided not to implement this replacement incident management tool.	None
8.2	28/02/07	Updated by N Bailey following review by HSD Tony Wicks updated POA contacts and escalation details.	None
9.0	27/04/07	Updated by Tony Wicks following formal comment cycle and issued for approval.	None
9.1	19/11/07	Name change POA to RMGA. POL BCM to Gary Blackburn. Updated risk table on related sections in the main body of the document, being: HSD switched to use of TfS for Incident Management. HSD DR site moved to BRA01. HSD primary site moved to STE04. Contact details updated	None
9.2	20/11/07	Minor changes and updates to the POL contact details. Issued for formal review cycle.	None
10.0	13/12/07	Comments incorporated for Gary Blackburn POL BCM, Liz Melrose and Paul Gardner. Issued for approval	None
10.1	30/01/08	N Bailey - Added SMC Doc ref / added SMC phone number / Notes about Tivoli PCs	None
10.2	20/05/08	N Bailey – updated after HSD BC Test / KMA / One Shot Password – Contact names	None
11.0	25/09/08	N Bailey – incorporated comments by T Wicks. Issued for approval	None
11.1	03/10/08	Revised by Tony Wicks for CP4772 Horizon Service Desk change of hours	None
12.0	20/11/08	Formally issued for approval after implementing comments received.	None

_

0.2 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks

Mandatory Review Authority	Name
Post Office Limited Business Continuity Manager	Gary Blackburn
Director RMGA Customer Service	Wendy Warham
CS Head of Service Management	Steve Denham
CS Service Delivery Manager (HSD)	Kirsty Gallacher
HSD Operations Manager (STE04)	Michael Jacklin
SMC Operations Manager	Ian Cooley
Optional Review / Issued for Information	
Core Services Business Continuity Manager	Nigel Bailey

(*) = Reviewers that returned comments

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 (RMGA) Incident Management Process	PVCS
REF7	CS/PRD/031			Fujitsu Services (RMGA) 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 - SMC
REF14	PROSMC038			Disaster Recovery for The Systems Management Centre	FSCS - SMC

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
BRA01	Fujitsu Bracknell site where HSD have a DR area
BCM	Business Continuity Manager
BT	British Telecomm
CMT	Communications Management Team (part of HSD)
DCS	Debit Card System
DR	Disaster Recovery
FMS	Field Maintenance Service
FSCS	Fujitsu Services Core Services Division
HSD	Horizon Service Desk
IMT	Incident Management Team (Part of HSD)
KMA	Key Management Access System
MBCI	Major Business Continuity Incident
MAC	Major Accounts Control Team
MIS	Management Information Service
NBX	Network Banking Service (the NBS Replacement service)
OBCS	Order Book Control Service
OOH	Out Of Hours
OSP	One Shot Password
PM	Post Master
POL	Post Office Limited
RMGA	Royal Mail Group Account
SDC01	Fujitsu Southern Data Centre - Number 1
SDC02	Fujitsu Southern Data Centre – Number 2
SLT	Service Level Target
SMC	Systems Management Centre
SOS	Systems Operate Service
SSC	System Support Centre
STE04	HSD – new primary site in Stevenage (Nov/07)
TfS	TRIOLE for Service – new Incident Management system used by HSD
UPS	Un-interruptible Power Supply

_

0.5 Changes in this Version

Version	Changes
11.1	Revised by Tony Wicks for CP4772 Service Desk change of hours and changed HSD Operations Manager to Michael Jacklin
12.0	Formally issued for approval after implementing comments received from Sarah Hill and Kirsty Gallacher.

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; 4, changes to bring this plan inline with the new contract. Changes will be required to this plan to reflect the introduction of additional DR capability for TfS in 2008.

0.7 Table of Contents

_

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).

–

3.0 OWNERSHIP AND OPERATION

The Fujitsu Services RMGA 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.
Kirsty Gallacher	CS Service Delivery Manager (HSD)	GRO	GRO
Tony Wicks	Fujitsu Services RMGA Business Continuity Manager.		
Richard Batty	Fujitsu Services Head of Service Desks		

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

4.0 FUJITSU SERVICES HORIZON SERVICE DESK FOR THE POST OFFICE

4.1 Introduction

This plan covers the following technical services:

Horizon Service Desk (HSD)

HSD is operational Monday to Friday from 08:00 to 18:30, and on Saturday from 08.00 to 14.00 and is comprised of four functional groups:

Front line Service desk staff:

This team takes calls direct from Post Masters or calls passed through from the NBSC

Incident Management Team (IMT)
This team effectively manage and report on any incidents impacting the desk, providing reporting for the customer and internally. This includes VIP sites/MI and DR instances. The team also measures all SLAs both contractually and internally.

Communications Management Team (CMT)
This team manage network issues with third party e.g., BT.

Major Account Controllers (MACs)
This group's role is to monitor and liaise with third parties who provide the engineering service. Specifically to escalate calls to the third party and provide a point of escalation to the end user.

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. TfS, is common to the HSD and SMC teams as an incident management system and by RMGA as a Problem Management system, these services are provided from a shared location at either SDC01 or SDC02.

4.1.1 Horizon Service Desk (HSD)

All calls are taken in STE04. 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
- 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, the 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 RMGA network to gain access to the TIVOLI management system.

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 (STE04).

The STE04 HSD site has a target ISDN30 bearer receiving Post Office Limited calls via BT Command Link. The STE04 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 STE04 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 BRA01, 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.

All calls diverted to the HSD disaster recovery site are directed to a direct dial number on the BRA01 Private Automatic Branch Exchange (PABX).

Remote diverts can be activated, by approved managers, via the Post Office Limited NBSC or, if OOH via the alternative contact point (refer to the HSD Contingency Process). This may need to be used in conjunction with the temporary transference of reinforcement staff from the inoperable centre to a DR site.

HSD uses a Fujitsu shared service for call management called Commander. This service utilises a multiple server configuration in STE04 which provides automated resilience in the event of a single server failure.

4.2.2 IT Systems TRIOLE for Service

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

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.

4.2.3 Electrical Power

To provide contingency against mains power failure, the HSD TfS system is covered by UPS and generators in SDC01, and the HSD 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.

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 RMGA contract. The nature of these tests is reflected in the Business Continuity Test Plan (REF4).

6.0 Preventative Measures

It is a fundamental philosophy of the RMGA 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 Service Desk to be delivered in part, or indeed in total, from one or more Service Desk 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 RMGA 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.

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 recognized 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 RMGA CS Service Delivery Manager or Duty Manager. The RMGA CS Service Delivery Manager or Duty Manager will use the RMGA Incident Management Process (REF6) to decide if a problem exists.

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

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

8.4 Initiation of recovery procedures

Where this is a RMGA only problem, recovery 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 problem within the relevant Service Level Target.

Depending on the severity of the problem, there may be some dialogue between the RMGA 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 RMGA 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 RMGA CS Service Delivery Manager or Duty Manager, for more involved problems the Duty or Problem Manager would liaise with the support teams, agreeing when the recovery action should be run, and then carrying out that activity.

–

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 RMGA project team have developed a vast knowledge of component failure and service availability over the life of the service.

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, RMGA, HSD**	(100% service requirement placed on BT via resilient systems, links contracted to POL not RMGA, therefore no contingency possible within RMGA) Log test calls / investigate Resolve via HSD 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 HSD incident management process.

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 RMGA, 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**
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, RMGA, POL**	Resolve via incident management process. Request MSS & SMC to assist. There are 25 PCs in STE04 for contingency. Consider partial relocation to the DR site where there are 3 Tivoli PCs **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**
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, RMGA and POL**	**For HSD:** Invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and RMGA 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**
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, RMGA and POL**	**HSD** must invoke command link to pass calls to voicemail. Consider assistance from associated SDUs, and RMGA Data Centres. Resolve via HSD incident process. **MBCI Go to 10.2.3** **Inform: POL BCT**

FUJ00080472

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.
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, RMGA 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

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 RMGA 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.	RMGA 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, RMGA, 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.	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	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.

					Business Impact: **HSD, RMGA, POL**	**Potential MBCI Go to 10.2.4** **Inform: POL BCT**
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, RMGA, 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**
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

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 STE04 for HSD

If STE04 (the primary site in Stevenage) is unavailable for use by HSD 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 RMGA Duty Manager is to arrange that all staff occupying HSD DR desks on the forth 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 HSD 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 PCs in STE04 that can be used for TfS, and other related services (including the MAC function), and forty PCs in BRA01.

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 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.

10.2.5 Loss Of access to Tivoli / KMA / 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), including the loss of any that may be available in the SMC, for an extended period of time (at least 3 hours) then temporary relocation to BRA01 shall be considered.

10.2.6 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.

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 RMGA 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 RMGA 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 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. 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 RMGA Business Continuity Management Process.

12.0 Contact List

12.1 Normal Processes

Organisation	Contacts	Telephone Number
Fujitsu Services RMGA	Duty Manager	Pager:
	CS Head of Service Management	Office: Mobile:
	CS Service Delivery Manager (HSD)	Office: Mobile:
(MBCI Contacts)	Business Continuity Manager	Office: Mobile:
	CS Senior Service Delivery Manager	Office: Mobile:
FS Core Services SOS Networks	Network Manager	Office: Mobile:
	Network Management Centre Manager	Office: Mobile:
FS Core Services SOS NT and UNIX	SOS NT and UNIX Manager	Office: Mobile:
	Technical Support Manager	Office: Mobile:
FS Core Services SMC	SMC Desk	Office 1 Office 2
	SMC Emergency shift phone	Mobile: GRO
	MSS / SMG Business Manager	Office: Mobile:
	SMC Operations Manager	Office: Mobile:
	Business Stream Manager	Office: Mobile:
FS Core Services HSD	HSD	HSD
	HSD STE04 Duty Manager	Mobile:
	HSD Operations Manager	Office: Mobile:
	Fujitsu Services Head of Service Desks	Office: Mobile:
Post Office Limited	Service Continuity Desk	Office:
	Business Continuity Manager	Office: Mobile:
	Systems Operations Manager	Office: Mobile:

12.2 Escalation Processes

Escalation Level	Level 1	Level 2	Level 3	Level 4
Fujitsu Services RMGA	CS Senior Service Delivery Manager Office: GRO	Problem Manager (Assigned by Duty Manager) BCM Office: GRO	Head of Service Management GRO	Customer Service Director Office: Mobile: GRO
FS Core Services Networks			Network Manager Office: GRO	NMC Manager : Office: GRO
SOS NT and UNIX			NT& UNIX Manager Office: GRO	Technical Support Manager Office: GRO
SMC			SMC Manager Office: GRO	Bus Stream Mgr Office: Mobile: GRO
HSD	HSD Duty Manager STE04 Duty Mobile: GRO	As per Level 1	HSD STE04 Ops Mgr Office: Mobile: GRO	Fujitsu Services Head of Service Desks GRO
Post Office Limited	Service Continuity Desk GRO		Business Continuity Manager Office: GRO	Systems Operations Manager Office: GRO