FUJ00080239

Document Title:	POA Operations Major Incident Procedure
Document Type:	Procedure Definition
Release:	HNG-X
Abstract:	This document describes the POA Operations Major Incident Management Procedure.
Document Status:	APPROVED
	This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager.
Author & Dept:	Tony Wicks– POA Operations
Internal Distribution:	As listed on pages 4 and 5 for Mandatory Review Optional Review Issued for information
External Distribution:	For information Dave Hulbert (POL), Steve Beddoe (POL), Antonio Jamasb(POL)
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Nana Parry	POA Tower Lead BAS	See Dimensions for record of approval.	

FUJ00080239

0 Document Control

0.1 Table of Contents

FUJ00080239

FUJ00080239

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	03-Oct-06	First draft – to detail the Major Incident Escalation process. Draft taken from Horizon Document CS/PRD/122, V1.0.	
1.0	11-Oct-06	Revision following comments from Reviewers	
2.0	02-Sep-08	Changes for Acceptance by Document Review: insertion of Section (0.4) containing table of cross references for Acceptance by Document Review and addition of note to front page. No other content changes.	
2.1	24-Feb-2009	Changes made for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes. Other changes to update Contact details.	
2.2	14-Apr-2009	Some Personnel Name changes and POA to POA + Abbreviations. Security Updates to sections 5.1, 6.3, 8.2.1, 9.0,	
2.3	3-June-2009	Some Personnel Changes and minor changes following review in May 2009	
3.0	7-July-2009	Following security audit 2 minor changes. Alan Simpson now on distribution and 6.3, an extra bullet entry added at end of list.	
3.0	7-July-2009	Following security audit 2 minor changes. Alan Simpson now on distribution and 6.3, an extra bullet entry added at end of list.	
3.1	14-Jan-2010	Changes following director failing to sign off v3.0, plus minor contact changes.	
4.0	26-Mar-2010	Approval version	
4.1	18-May-2010	Following team restructure, the process has been significantly reviewed.	
4.2	03-Jun-2010	Updated following minor comments provided during review cycle of version 4.1. This version will be presented for approval at v5.0	
5.0	07-Jun-2010	Approval version	
6.0	14-Sep-2010	Approved version following updates to personnel and table in 10.4 and section 10.8	
6.1	15 July-2011	Updates to personnel and changes from 'Process' to Procedure'	
6.2	05-Sept-2011	Updates following changes requested by Bill Membery from 6.1, plus clarification of TRM role	
6.3	14- Oct- 2011	Cosmetic changes mainly changing RMGA with POA and also updating abbreviations	
6.4	21-Dec-2011	Updating of details for a Service Bridge. Also some POL requests. Despite this being an internal POA document, all external comments that can improve the document are considered.	
6.5	16-Jan-2012	Updated, following review and cosmetic changes in relation to version 6.4	
7.0	02-Jan-2013	Changes in relation to Personnel and also Tower Leads and other cosmetic changes	
7.1	04-Feb-2013	Changes in relation to Personnel and revisions around Communications	

FUJ00080239

7.2	17-Sep-2013	Major update to align with Business Assurance Management procedures and for organisational changes. (This version was originally identified as version 8.1)	
8.0	18-Oct-2013	Updated for minor changes from Nana Parry.	

0.3 Review Details

Review Comments by :	04/10/13
Review Comments to :	Tony Wicks

Mandatory Review	
Role	Name
POA Tower Lead BAS	Nana Parry
POA Acceptance Manager	David Cooke
POA Lead Problem and Major Incident Manager	Steve Bansal
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andrew Hemingway
POA Business Continuity Manager	Sathish Ramalingam
POA POLSAP and Online Services SDM	Gaby Reynolds
POA Credence and Sales force SDM	Victoria Hancock
POA Problem Manager	Stephen Gardiner
POA Lead SDM End User Services	Leighton Machin
POA Lead SDM Online Services	Yannis Symvoulidis
POA Senior Ops Manager HNS	Alex Kemp
Fujitsu HSD Operations Manager	Mike Clive
POA SMC Manager	Catherine Obeng
POA Security Manager	Kumudu Amaratunga
POA SDM HSD	Sandie Bothick
POA Quality Compliance and Risk Manager	Bill Membery
POA Network Infrastructure SDM	Roger Stearn
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
POA CISO	Brad Warren
POA Unix Team Leader	Fiona Lennox
Fujitsu NT Team Leader	Ian Gibson
Fujitsu DC Operations Manager	John Hill

(*) = Reviewers that returned comments

0.4 Acceptance by Document Review

The sections in this document that have been identified to POL as comprising evidence to support Acceptance by Document review (DR) are listed below for the relevant Requirements:

FUJ00080239

POL NFR DR Acceptance Ref	Internal FS POL NFR Reference	Document Section Number	Document Section Heading
SER-2200	SER-2178		Whole Document
SER-2202	SER-2179		Whole Document
SEC-3095	SEC-3266	3.3.5	Security Triggers
SEC-3095	SEC-3266	10.5	Security Major Incidents

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Royal Mail Group Account HNG-X Document Template	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	Dimensions
SVM/SDM/SD/0025			POA Problem Management Procedure	Dimensions
PA/PRO/001			Change Control Process	Dimensions
CS/QMS/001			Customer Service Policy Manual	Dimensions
SVM/SDM/SD/0001			Service Desk – Service Description	Dimensions
266/FRM/HSD/001			HSD Business Continuity Activities Plan	Dimensions
SVM/SDM/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0030			HNG-X Engineering Service Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			HNG-X Security Business Continuity Plan	Dimensions
SVM/SDM/SD/0011			Branch Network Services Service Description	Dimensions
SVM/SDM/PRO/0018			CS Incident Management Procedure	Dimensions
C-MSv1.3			Manage Incidents Process	BMS
C-MSv_roles			Service Management Process Roles and Responsibilities	BMS
SVM/SEC/STD/1823			LINK information security standard issued January 2001 (subject to such dispensations from that standard as LINK may grant from time to time).	Dimensions
IM002_MAJOR INCIDENT MANAGEMENT PROCEDURE	5.0	23/05/2013	Manage Major Incidents Procedure	BMS
FJ- BMS- 1-AB1.6	6.0	24/04/2012	Fujitsu Services Business Management Systems Process: Conduct Root Cause Analysis	BMS

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

FUJ00080239

0.6 Abbreviations

Abbreviation	Definition
A+G	Advice & Guidance
BCP	Business Continuity Plan
BMS	Business Management System
HSD	Horizon Service Desk
IMT	Incident Management Team
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEDB	Known Error Database
KEL	Known Error Log
MBCI	Major Business Continuity Incident
MIM	Major Incident Manager
MICM	Major Incident Communications Manager
MIR	Major Incident Report
MSC	Manage Service Change
MSU	Management Support Unit
OCP	Operational Change Proposal
PCI	Payment Card Industry (as per Security Standards Council)
PO	Post Office
POA	Fujitsu Post Office Account
POL	Post Office Limited
RFC	Request For Change
SCT	Service Continuity Team
SDM(s)	Service Delivery Manager(s) (NB: Throughout this document SDM refers to a person responsible for the Service, and the SDM could work in, but not limited to, the Service Delivery, Service Support, and Release Management or Security teams).
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SMS	Short Message Service (as known globally within Mobile Telephone Networks)
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
TB	Technical Bridge
TP	Third Party or Third Parties
TRM	Technical Recovery Manager
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

FUJ00080239

Term	Definition
T	Time of incident occurring
T+3	Time Incident Occurred plus 3 minutes

0.8 Changes Expected

Changes
Changes to reflect process and organisational changes. This is expected to be changed for the OSR Messaging release.

0.9 Accuracy

Fujitsu Services endeavours to ensure that the information contained in this document is correct but, whilst every effort is made to ensure the accuracy of such information, it accepts no liability for any loss (however caused) sustained as a result of any error or omission in the same.

0.10 Security Risk Assessment

Security risks have been assessed and it is considered that there are no security risks relating specifically to this document.

FUJ00080239

1 Introduction

1.1 Owner

The owner of the Major Incident Management process at the local POA level is the Fujitsu POA Lead SDM, Problem and Major Incident.

Objective

The key objective of the procedure is to ensure effective and efficient management of Major Incidents, through:

- Improvement of communication channels
- Clarification of the need to communicate awareness of potential incidents
- Improved accuracy of reporting of incident status
- Allowing technical teams the right amount of time to diagnose and impact an incident
- Avoiding unnecessary alerting of the customer
- Demonstrating a professional approach to the Post Office
- Provision of clearly defined roles and responsibilities
- Defined reporting and updating timelines throughout a major incident.
- Improved governance
- Assessing which incidents are major and which are 'Business as Usual'

1.2 Rationale

This document outlines the communication and management procedure and guidelines to be used for Major Incidents impacting the live estate.

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

The aim of the document is to provide a pre-defined procedure for future major incident communication and management.

FUJ00080239

2 Mandatory Guidelines

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) Avoiding unnecessary alerting of the customer

c) Assessing which incidents are major

The following guidelines should be adhered to.

- During the HSD IMT Core Hours (Monday – Friday 07:00 – 19:00 and Saturday 08:00 – 14:00) the HSD IMT should be the first point of operational contact between Fujitsu and the end user. Outside these hours the HSD Telephones will be diverted to FJ Wakefield from 19:00 to 23:00 weekdays, Saturday 14:00 – 23:00 and Sunday 08:00 – 17:00 whilst SMC can also be contacted 24 x 7 x 365.
- Any activity detailed in this document which is assigned to the HSD IMT is handed over to the SMC outside the HSD IMT Core Hours, with the exception of the above.
- The relevant technical teams who are aware of and monitoring a potential major incident must page / call the appropriate Major Incident Manager (Duty Manager out of hours) as ***soon as possible.*** This is not limited to major incidents alone, but applies wherever a state other than Business as Usual has been detected. The Major Incident Manager must in turn communicate the potential incident, to the POL Service Desk for awareness and monitoring in POL. This is usually done via the HSD IMT in core hours or via SMC out of hours.
- The Major Incident Manager (or Duty Manager out of hours) is responsible for communicating both *up* the Fujitsu organisation and *across* (see appendix 10.3) to their counterpart in POL. Where this is impractical (e.g. leave, out of hours, unavailable), the initiative should be taken to jump up the organisation. Of prime importance 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, likely impact, and the Fujitsu owner to contact.
- The Major Incident Manager (Duty Manager OOH, who covers Monday to Friday 17:30 to 09:00 and from 17:00 Friday though to 09:00 Monday) should also initiate communication using SMS via the HSD IMT (07.00 to 19.00 Monday to Friday, and Saturday 08.00 to 14.00). Outside of these hours the SMS should be via the SMC. The SMS distribution list used is titled 'SMS Internal' and amongst others includes the appropriate members of the POA Operations Management Team.

FUJ00080239

3 Definition of a Major Incident

3.1 Incident Classification

As a general rule a Major Incident will be an incident rated as a Business Critical Incident as shown in the following

- The 'CONTRACT'
- Sections 3.2 and 3.3 below.
- POA Operations Incident Management Procedure document (SVM/SDM/PRO/0018).
- A series of connected lower severity incidents which combine to have a significant business impact.

However not all incidents rated as Severity 1 qualify as a Major Incident as the severity levels do not always reflect the overall business impact to POL. For example a single counter post office which is unable to trade, regardless of its business volumes, is rated as a Severity 1 incident.

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 contained 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 in calling a Major Incident

It is important that a Major Incident is defined in accordance with section 3.3 Major Incident Triggers, 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. However the following parameters will also feed into the consideration of whether a major incident should be called:

- 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
- Time of year – e.g. Christmas / Easter / End of month / quarter
- Anticipated time before service can be resumed
- Impact to POL branches, customers, clients or brand image
- Business initiatives e.g. product launches

3.3 Major Incident Triggers

The following criteria could trigger a major incident, however as detailed in 3.2, the influencing factors must also be considered. As such the list below is not exhaustive, whilst if an incident occurs which is not detailed below, e.g., legislative, it should not necessarily be precluded from being declared a major incident.

It should be noted that any call trends in relation to the following, should be reported to the POA Duty Manager as soon as the agreed threshold levels have been breached.

FUJ00080239

3.3.1 Network Triggers

Network Major Incident triggers are as follows:

- Complete or significant outage of the Central network, e.g. failure of both 3750 stack Catalyst switches in totality for the Core layer in IRE11.
- Complete or significant outage of the Talk Talk network
- Complete or significant outage of VSAT sites
- Complete or significant outage of the ISDN network (whether C&W, BT or Kingston Comms)

3.3.2 Infrastructure Components Triggers

Infrastructure component Major Incident Triggers are as follows:

- Total loss of environments providing individual online service capability
- Breach of access to data centres
- Breach of security
- Virus outbreak

3.3.3 Data Centre Triggers

Data Centre Major Incident triggers are as follows:

- Network / LAN outage
- Loss of Data Centre, or significant loss of Data Centre Components
- Breach of security

3.3.4 Online Service Triggers

Online services Major Incident Triggers are as follows:

- Online service unavailable within the Data Centre (not counter level)
- Number of Branches without Communications Services – as defined by POL and in accordance with Ping script thresholds.
- Third party provided service failure – e.g. DVLA, Link, Moneygram, Santander etc

  N.B Once the third party service provider has been deemed to be the source of the Major Incident; it will be managed by either POA or POSD in accordance with whichever organisation manages that supplier relationship.

3.3.5 Security Triggers

Security major incident triggers are as follows:

- Actual or suspected attacks on the Fujitsu Services Buildings and its resources, POA Network or Information Systems
- Theft of IT equipment / property, and in particular PIN Pads
- Theft of software
- Any PIN Pad Issues that are in breach of FIPS 140-1 level 3 and ISO 9564 1st Edition 1991 section 6.3.1 as specified in the LINK information security standard issued January 2001 (subject

FUJ00080239

to such dispensations from that standard as LINK may grant from time to time). The main criteria being as follows:

> *The purpose of this Standard is to protect the LINK Network, its Members and their cardholders and ATM owners from attacks designed to compromise sensitive data or defraud financial institutions and their cardholders. This protection takes into account not just the direct financial losses that may be incurred but also the potential reputational damage to the LINK ATM Scheme and its Members and its impact on customer confidence in LINK and ATMs in general. It is intended to protect the Link Brand:*
>
> - *The interests of the Members*
> - *The interests of the Members' customers*
> - *The reputation and integrity of the UK cash handling infrastructure*

In the event of a Security Major Incident (which may also include PCI Incidents), the POA Security Manager MUST be alerted who will then follow the Security Incident Management processes, as detailed in both:

SVM/SDM/PRO/0018 Appendix A

SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan (defines the actions to be taken if security violations are identified).

In the event of a Major Incident Security trigger for Fujitsu Services Buildings and its resources, the POA Security Manager MUST inform the Group Property Security Team who will be alerted either by telephone on a 24/7 basis or the next working day via our Incident Reporting process and the actual or potential impact of the incident dictates which route is followed.

The Group Property Security Team will then take responsibility for interfacing into the corporate process by entering reports on to the corporate system.

FUJ00080239

4 Security Major Incidents

In the event of a security major incident, the incident procedure as detailed in the POA Customer Services Incident Management Procedure (SVM/SDM/PRO/0018 Appendix A) must also be followed.

SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan defines the actions to be taken if security violations are identified.

FUJ00080239

5 Calling the Major Incident

During business hours the Major Incident Manager declares and manages the Major Incident (with handovers to the POA OOH Duty Manager where applicable.)

Where the impact of the incident is not immediately obvious, and it is not clear if a Major Incident should be called, escalation and discussion with the POA Operations Management Team should occur, and a collective decision made. If a Major Incident is not called, the incident should be monitored until closure, to ensure that the impact does not increase to that of a Major Incident.

In the event that multiple services are impacted, multiple Major Incident Managers may be appointed by any Tower Lead and will remain in their roles until incident closure.

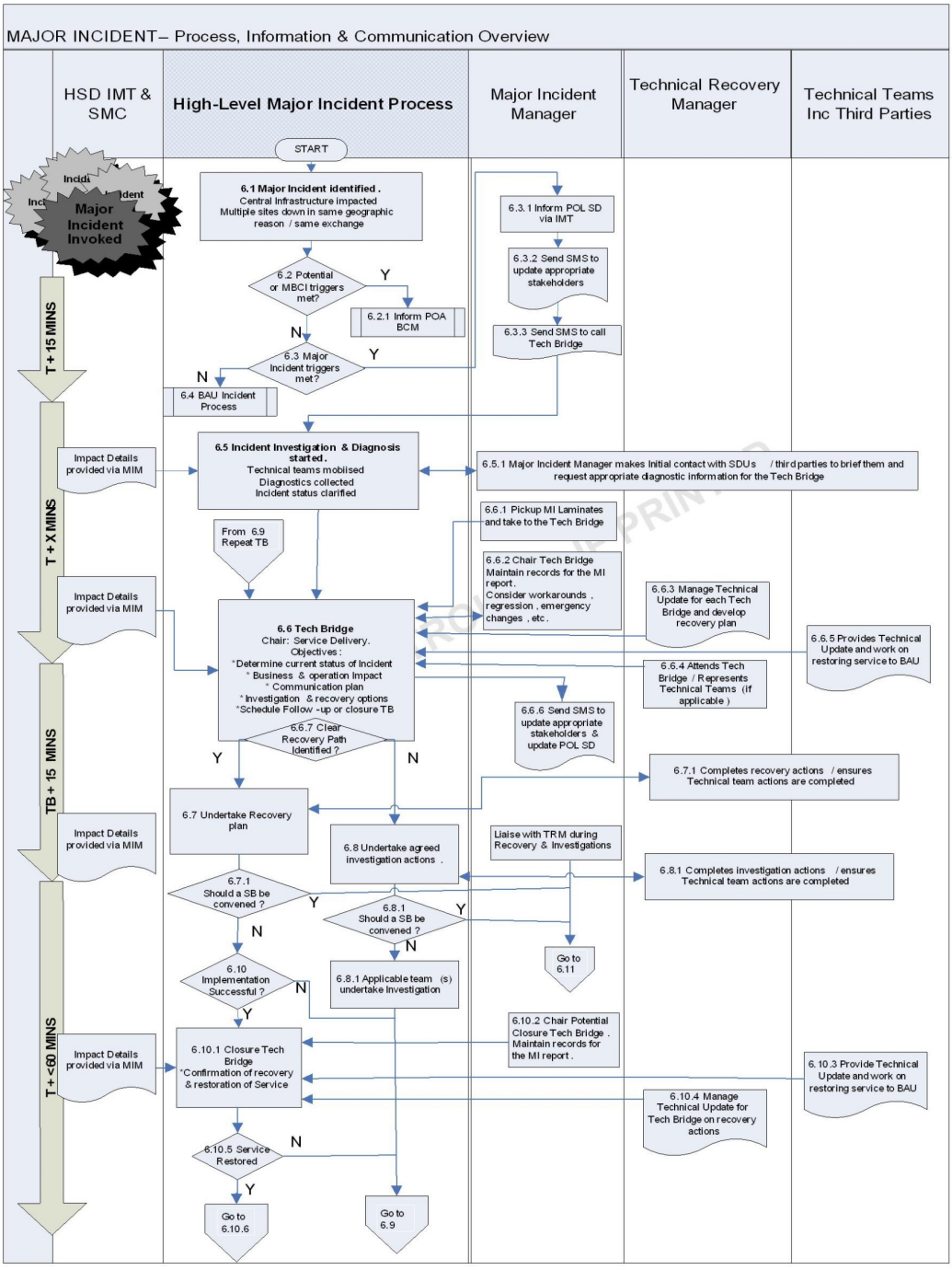
Out of hours the POA OOH Duty Manager is responsible for declaring a Major Incident.

Section 9 of this document specifies the roles and responsibilities during a major incident. The Major Incident Manager, see section 9.2, is referred to the Manage Major Incident Procedure and must endeavour throughout the life of a major incident to adhere to the principles of that procedure.

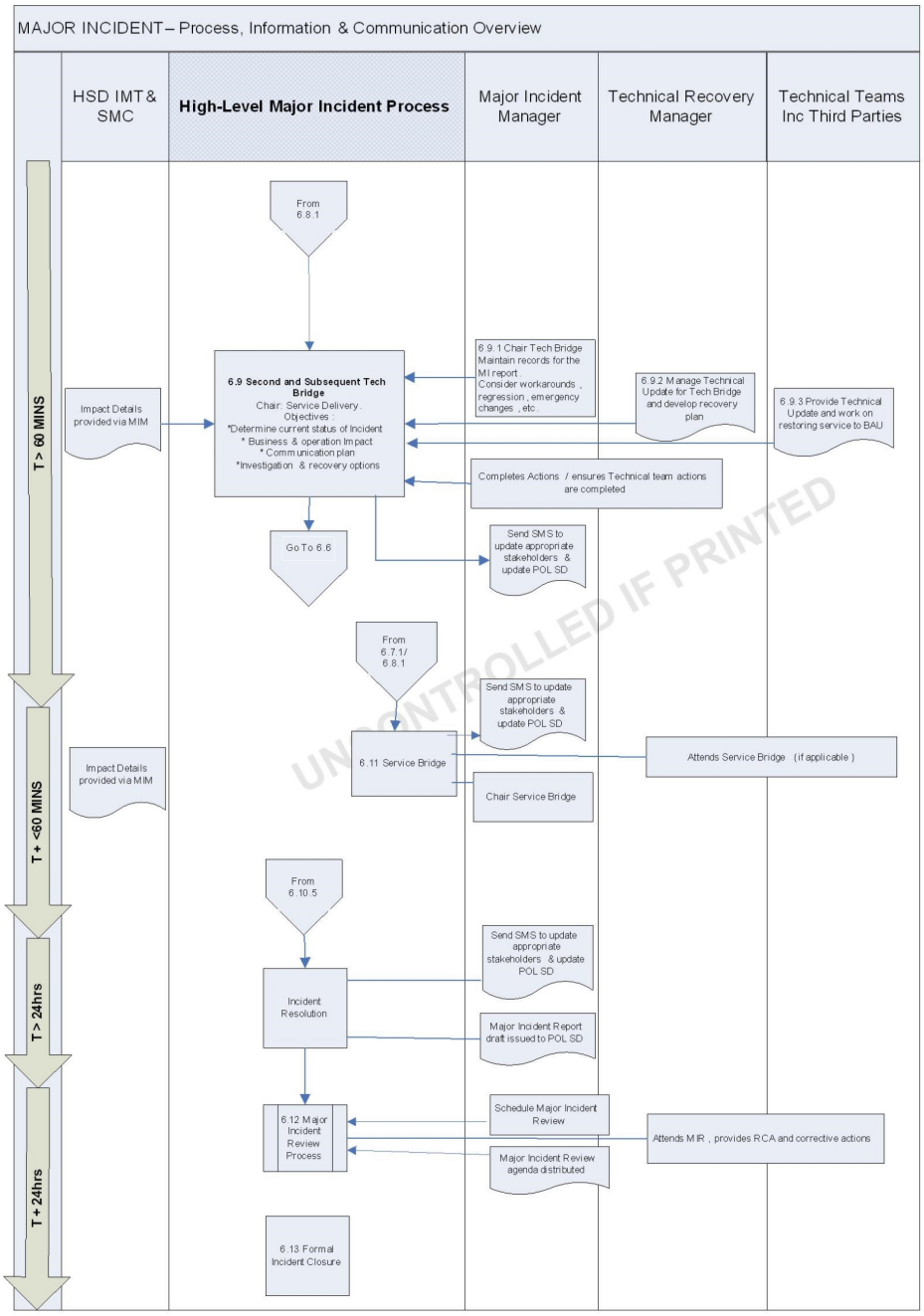
FUJ00080239

6 Process Flow

FUJ00080239



FUJ00080239



FUJ00080239

6.1 Process Description

Process ID	Box Title	Description	Key timescales	Accountable/ Responsible	Outputs/ Inputs
6.1	Major 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." (SVM/SDM/PRO/0018). An incident may be reported from within POL domain, a supplier domain or other route			
6.2	BC Incident?	The Major Incident Manager will consult with the Business Continuity Plans (see section 0 of this document) to identify if the potential MBCI or MBCI triggers have been met, and inform the POA Business Continuity Manager if appropriate.	T+3	POA Duty Manager (A)	Escalation as a MBCI or Potential MBCI is undertaken if required. (O)
6.3	Major Incident Triggers Met?	An initial impact assessment of the incident is undertaken by members of the POA Service Team taking into account impact on: Live Service, Financial Integrity, Business Image. Refer to Section 3 of this procedure. If the incident is profiled as a Major Incident, including consideration of influencing factors, e.g. time, geographical coverage, business impact, security, public perception, duration and relevant business initiatives coinciding at POL then go to 6.3.1 If the incident does not meet the Major Incident criteria go to 6.4.	T+3 All timescales quoted are 'best endeavours' and are dependent upon circumstances T+5	Major Incident Manager (A)	Major Incident Manager assigned (O)
6.3.1	Initial Communication	The POL Service Desk will be informed by the IMT or Major Incident Manager of the incident, and this will also be escalated to POA Service Management / POA Service Operations team managers, if this has not already been done. In the event of either a potential Major Incident or a Major Incident in its own right, the POA Major Incident Manager will escalate to the POL Live Service Manager and advise accordingly.		Major Incident Manager (A)	Potential Major Incident advised. (O)
6.3.2		With agreement from the POA SDM for the affected service, or the Duty		POA SDM or	SMS sent when

FUJ00080239

		Manager out of hours, an SMS will be sent to POA and POL Management alerting to the potential existence of a Major Incident.		POA Duty Manager(A)	agreed (O)
6.3.3		POA Service Operations Manager or POA Duty Manager to send out an SMS calling a Tech Bridge with a brief synopsis of the MI and Tech Bridge phone details. Go to 6.5.		POA Ops Mgr/POA Duty Manager (A)	SMS sent calling TB. (O)
6.4	BAU Incident Procedure	If a Major Incident is not declared then the BAU Incident procedure is followed – the POL Service Desk will be informed that there is no Major Incident and an SMS sent to the POA Management Team. The POA SDM for the service should ensure that the Incident is re-impacted during its lifecycle to ensure that the impact has not increased. If, subsequently the incident is declared a Major Incident, go to 6.5.		POA Duty Manager (A)	POLSD advised. SMS sent to POA Management(O)
6.5	Major Incident Investigation & Diagnosis		T+ 5		
6.5.1		Relevant internal SDUs / Third Parties contacted to initiate investigation and diagnosis. Attendees at the Tech Bridge may include POA Service Management, SDUs, Third Parties, POA Operations Security Technical teams mobilised, diagnostics requested, further clarification on the MI and symptoms, etc.		Major Incident Manager (A)	Initial contact with SDUs & Third Parties. (O)
6.6	**Tech Bridge**		T+10		
6.6.1	Tech Bridge	Before commencing the first and subsequent Tech Bridge calls, the Major Incident Manager is to pickup the Major Incident Laminates from outside the POA 'Parcel Room' or from the desk of the Lead SDM for Problem and Major Incidents.		Major Incident Manager (A)	MI Laminates available for TB. (Input)
6.6.2	Tech Bridge	Once confirmed as a Major Incident the Major Incident Manager must ensure that the information required for the Major Incident Report is captured. See section 10.1 for details of the template. The Tech Bridge agenda which covers: **Roll call, Summary / Overview of Incident, Current Impact, Investigation / Recovery Action, Remedial**	T + 15	Major Incident Manager (A)	The information required to progress the MI investigation, provide updates

FUJ00080239

		Actions, Actions to carry forward to Major Incident Review During the Technical Bridge the MIM and TRM must consider if any of the following are required and invoke applicable POA local procedures The need for a Problem Record Potential work around activities A normal or emergency change. Sufficient details to populate both the Major Incident Progress Template and Report Template Consider if a Problem Record is required or if the major incident could potentially be resolved via a work around or planned change			and maintain records for MI report. (O)
6.6.3 & 6.6.4	Tech Bridge	The Tech Bridge is chaired by the Major Incident Manager with assistance from the Technical Recovery Manager (TRM). The TRM is to ensure that the Technical Bridge aims are met as follows: • To discuss and agree the recovery, investigation and resolution of the Major Incident • To provide a forum for up-to-date progress reports • To aid communication and support the MIM to produce a short term technical recovery plan and if appropriate longer term corrective actions. These will be included in the Major Incident report.		Technical Recovery Manager/All (R) Major Incident Manager (A)	
6.6.5	Tech Bridge	Where a Major Incident could be as a result of a Third Party, or require their assistance in rectifying the issue, there input will be required in the Tech Bridge		Third Parties (As applicable)	Technical Support (I)
6.6.6	Tech Bridge	If the outcome of the Tech Bridge 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 SMS communication, including both timing and delivery requests, becomes the responsibility of the Major Incident Manager. NB 30 minute updates should be the norm unless otherwise requested by	Tech Bridge + 15	Major Incident Manager (A)	Provide an SMS update. (O)

FUJ00080239

		POL The Major Incident Manager will also distribute recovery actions (provided by the TRM), during the conference call. At the time agreed at the first Tech Bridge, subsequent Tech Bridges are held as required. The same agenda is followed, and progress on actions / recovery is provided. If no clear recovery path is identified, the decision is then taken on whether to escalate for Service Bridge direction. (Invoking a Service Bridge)		Technical Recovery Manager (a) Major Incident Manager/ Technical Recovery Manager (A)	Distribute planned recovery actions. Decision on need for a Service Bridge. (O)
6.6.7	Tech Bridge	If during the Tech Bridge a clear recovery path is identified, this should be discussed and agreed alternatively further diagnostics and evidence will be required. Schedule a follow-up Technical Bridge to co-inside with either the completion of the recovery activities, if these are expected to be completed within one hour, or at appropriate 'touch-points' agreed with the Technical Recovery Manager, for recoveries that cover an extended duration. For recovery go to 6.7 and for further investigation go to 6.8.		Technical Recovery Manager (A) Major Incident Manager (A)	Define diagnostic evidence required. (O) Next Technical Bridge time agreed. (O)
6.7	**Recovery**		T + x		
6.7.1	Recovery	The Technical Recovery Manager will liaise with the SDUs and /or third parties during the recovery. Where appropriate technical conference calls may be arranged for technical discussions between SDUs and if applicable Third Parties. The TRM is to advise the MIM if it is considered that the Recovery has been successfully completed. The MIM is to call the MI Closure Tech Bridge. Go to 6.10.		Technical Recovery Manager (A)	Co-ordinating and Managing the Recovery process. (O) Advising the MIM to call the MI Closure Tech Bridge (O).
6.7.2	Recovery	After the MI has been in-progress for one hour the MIM is to consult with POA Service Management to ascertain if a Service Bridge is required. See 6.11 for Service Bridge details.	>T+ 60	Major Incident Manager (A)	Decision on holding Service Bridge (O)

FUJ00080239

6.8	**Investigation**		T + x		
6.8.1	Investigation	The Technical Recovery Manager will liaise with the SDUs and /or third parties during the MI investigation. Where appropriate technical conference calls may be arranged for technical discussions between SDUs and if applicable Third Parties. The TRM is responsible for ensuring that the SDUs and Third Parties obtain the agreed evidence to enable subsequent Technical Bridges.		Technical Recovery Manager(A) SDUs and Third Parties (R)	Diagnostic information, event logs, test results, as applicable (I)
6.8.2	Investigation	After the MI has been in-progress for one hour the MIM is to consult with POA Service Management to ascertain if a Service Bridge is required. See 6.11 for Service Bridge details.	>T+ 60	Major Incident Manager (A)	Decision on holding Service Bridge (O)
6.9	Tech Bridge 1+ (in the event of multiple MI's)	This procedure will be followed as per instructions, irrespective of how many MI's are running. After the time agreed in section 6.6.7 the next Technical Bridge is to start. All SDUs investigating the MI are to take the evidence they have obtained following their investigations. The MIM is to go to step 6.6 and ensure that they have copies of the Major Incident Laminates to record the further details.		Major Incident Manager/ Technical Recovery Manager (A)	Individual Major Incident Reports for individual Major Incidents.(O)
6.10	**MI Closure Tech Bridge**		T+X		
6.10.1	MI Closure Tech Bridge	Once the incident is deemed to be resolved, a final Post Incident Review (PIR) Technical Bridge is to be arranged to review the Major Incident.		Major Incident Manager (A)	SMS sent confirming that the Major Incident has been resolved and the action taken to resolve it. (O)
6.10.2	MI Closure Tech Bridge	The MIM is responsible for producing a Draft Major Incident Report and distributing this within one working day of resolution of the Major Incident. Therefore the MIM must ensure the results of this closure technical bridge are documented.		Major Incident Manager (A)	Produce the minutes of the Closure Technical Bridge (O)
6.10.3	MI Closure	The SDU and Third Parties are to provide updates on the actions taken to		Major Incident	Actions

FUJ00080239

	Tech Bridge	restore service and confirm that all actions have been completed and that the affected end service has been restored.		Manager (A) SDUs & TPs (R)	Completed, Service Restored (I)
6.10.4	MI Closure Tech Bridge	The MIM, in conjunction with the TRM, is to confirm that service has been restored and the MI resolved. For resolved MIs go to 6.10.5 If there is any doubt about the status of the MI it shall still be considered Open and a further Tech Bridge is required. Go to 6.6		Major Incident Manager (A)	MI Resolved Decision (O)
6.10.5	MI Closure Tech Bridge	The MIM is to send an SMS communication confirming resolution of the incident. The MIM is to produce the draft report which is to be sent to POL within one working day and a formal version 1.0 of the report within seven days.		Major Incident Manager (A)	SMS sent providing agreed resolution details. (O) Draft MI Report Within one working day (O)
6.11	Service Bridge	The nature of the incident determines which POA Service Team members and POL Managers are involved in the Service Bridge but it would include **all or some** of the following: • POL (personnel as instructed by POL Live Systems Service Mgr) • POA Tower Lead BAS (Chair Person) • POA Other Tower Leads • POA Lead SDM, Problem and Major Incident • POA Business Continuity Manager • POA Security Manager • POA SDM owning the affected service • POA Technical Recovery Manager • Third Party Executives (if appropriate) • Appointed working group representatives as appropriate	Timescale dependant upon impact and nature of incident.	Major Incident Manager (A) POL Service Manager	Relevant decisions and information from the Service Bridge(s) is to be included in the Major Incident Report. (O)

FUJ00080239

		• HSD IMT Representative The purpose of the Service Bridge is to: • Provide appropriate direction on incident resolution • Improve communications across Third Party business boundaries and enable senior management in the respective organisations to address any factors impeding a more timely resolution. • Provide added impetus to restoration of service as quickly as possible • Define communication intervals to key stakeholders • Provide focused incident management in line with the impact and severity of the incident			
6.12	Post Incident Review & formal Incident Closure	Hold a Post Incident Review of the Major Incident. Note there is no predefined time in which the PIR is held as it is dependant upon follow-up actions including Problem Records being addressed. Refer to section 8.0 for further details and give consideration to the following: • Lessons learnt • Incident definition • What went well • Timeline • Changes required to the infrastructure • A review of the Major Incident communications • Root Cause Analysis (if known at this point) • Business impact • Action plan, including any changes requiring MSCs • Service Improvement Plan update • Review any service risk(s) and update the Risk Register as appropriate		POA Lead SDM, Service Operations (A)	Finalise the Major Incident Report (using the output of the PIR). (O)

FUJ00080239

6.13	Formal Closure	All remedial actions completed both short and long term. Including root cause analysis, and also reviewing/closure with POL all associated Problem Records, including POL signing off the Major Incident.		POA Lead SDM, Service Operations (A)	All PIR actions completed. (O)

Note: Within 'Key Timescales' the reference made to T, = Time of incident occurring. hence T+3 = time incident occurred plus 3 minutes.

FUJ00080239

7 Communication

7.1 Technical Bridge

This is a Fujitsu technical conference for Technical experts and SDU's to discuss and analyse the incident and to formulate an action plan to restore the service to POL without delay. It should enable the Technical Recovery Manager to baseline the anticipated response, covering resolution, time and resources required. This will also include the appropriate owning SDU of the service affected by the Major Incident.

The Technical Bridge will be set up as required by the Major Incident Manager.

Invitations to the Technical Bridge will be via SMS, email or voice. The SMS will be sent to the distribution list titled '**SMS Technical Bridge**'. The SMS text will be sent to all technical experts on the POA and will include outline details of the Major Incident. Also dial in details and the start time will be provided as part of the meeting invitation.

The Technical Bridge will be started at T + 15, and reconvened at regular intervals during the Major Incident; the exact scheduling will be discussed and agreed at each preceding Major Incident Call.

Each Technical Bridge follows a set agenda which will be distributed with the meeting invitation where possible. The conference call is chaired by the Major Incident Manager with the recovery managed by the Technical Recovery Manager.

A request for a Technical Recovery Manager (TRM) will be made to the appropriate Tower Lead, who will appoint one of his team to be the TRM.

Following each Technical Bridge, it is the responsibility of the TRM to publish any actions as follows

-Recovery / restoration actions (which should normally include associated MSC numbers),

-Service Improvement Plan recommendations

-Risk Register recommendations

-Recommendations for any improvements to KELS / Alerting / Configuration changes

The above will be documented in the Major Incident Report and stored on: **IRRELEVANT** under Service Support > Major Incident Reports.

FUJ00080239

7.2 Service Bridge

This is a service focussed call for Service Management (including the Technical Recovery Manager if appropriate) and POL to discuss the service impact of the Major Incident and to receive updates on the progress towards resolution.

The purpose of the Service Bridge is to provide a focussed area from which strategic decisions can be made regarding a Major Incident.

Attendance is made up of the following or their designated representative:

- POL (Personnel as instructed by POL Live Systems Service Manager)
- POA Tower Lead (Chair Person)
- POA other Tower Leads
- POA Lead SDM, Problem and Major Incident
- POA Business Continuity Manager
- POA Security Manager
- POA SDM owning the affected service
- POA Technical Recovery Manager
- Third Party Executives (if appropriate)
- Appointed working group representatives as appropriate
- HSD IMT Representative

Service Bridge responsibilities include:

- Agreement of a containment plan
- Documentation of all agreed actions and timescales with owners
- Consistent management of the Major Incident across all the locations involved
- Management of potential Major Business Continuity Incidents (MBCI's) within POL and the POA
- Co-ordinate meeting times and locations

In the event of a Major Incident requiring a Service Bridge, it is envisaged that this will be in place at T+60 (or earlier if required by POL). Participants required in the Service Bridge will be contacted via SMS as appropriate.

A POA Tower Lead will send out a text via IMT in order to organise a Service Bridge.

Invitations to the Service Bridge will be via SMS, email or voice. The SMS will be sent to the distribution list titled '**SMS HNGX External'**

The SMS text should state such details as;

- An outline of the ongoing incident,
- Dial in details
- Start time.

e.g. 'Your attendance is required at a Service Bridge to discuss the current Major Incident in relation to Online Services. Please call GRO or GRO Participant code: ####### at 11.00 hrs.'

The chairperson's code is held by the POA Tower Leads and the Problem and Major Incident Managers. The chairperson, normally the POA Tower Lead will initiate the call.

FUJ00080239

The TRM will attend meetings as required and provide appropriate root cause analysis and corrective action detail.

FUJ00080239

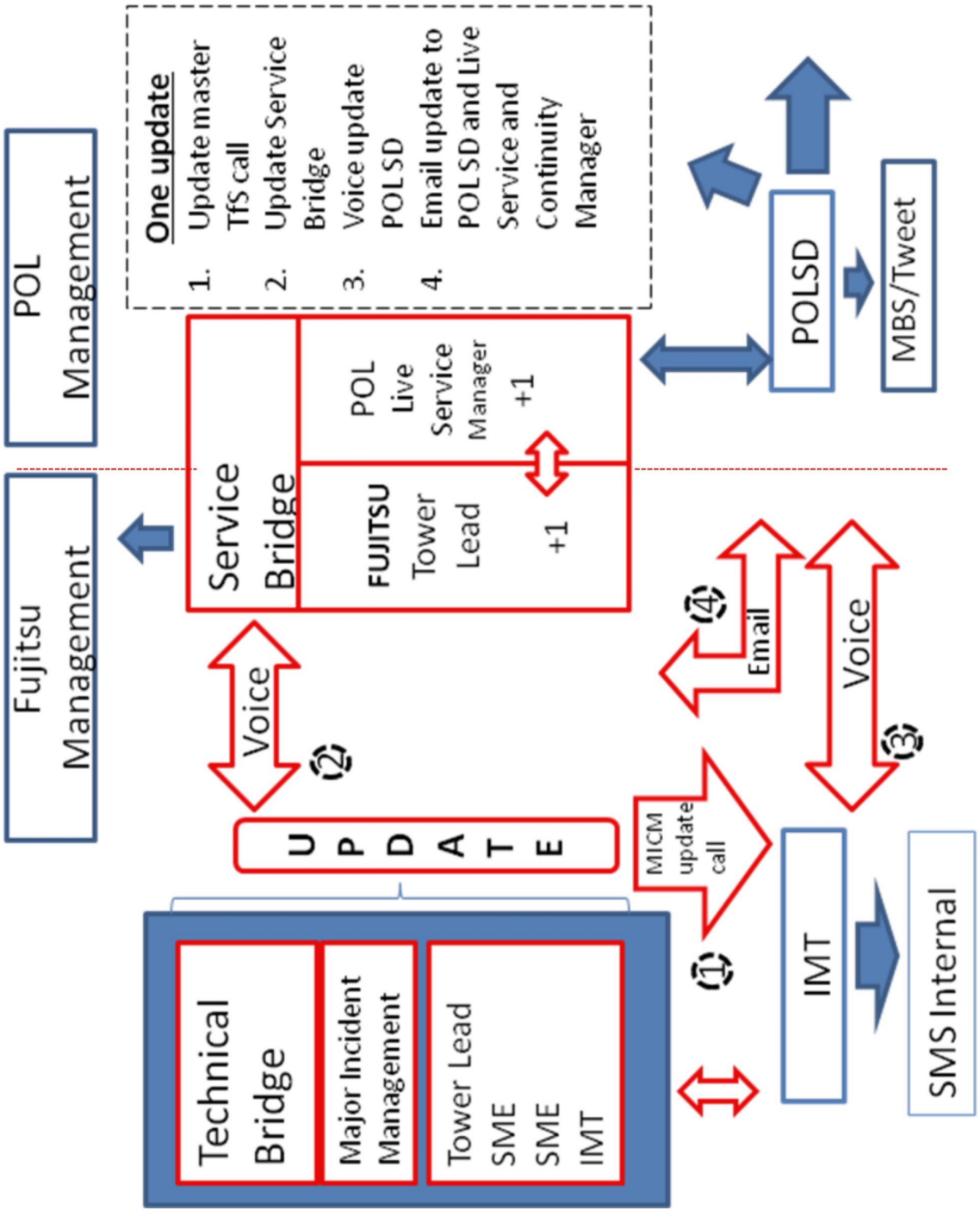
7.3 Communication Process Flow

- On suspicion or confirmation of a Major Incident, the MIM will escalate to the Lead SDM for the area, Problem and Major Incident Management SDM, and to the POA Tower Leads.
- The MIM will inform the POL Service Desk, via the HSD IMT, of the start of the service incident alerting of potential issues – including date, time, nature of problem, severity and impact if known and then directly inform the POL Live Service Manager
- All updates to the POL Service Desk are via the HSD IMT, within agreed timescales controlled by the MICM
- The MICM will issue an SMS text to the POA via the HSD IMT, alerting of potential issues – including date, time, nature of problems, severity, impact and name
- A POA Tower lead will inform the following within 10 minutes of start of the service incident
  - POA Delivery Executive
  - POL Senior Service Delivery Managers

  And will coordinate and ensure consistency of response to POL and POA Senior Management via The Service Bridge
- Periodic (interval to be determined depending on the nature of the issue but not more than 30 minutes for Major Incidents) SMS updates to be sent to the original SMS Dist list
- On final service restoration, an SMS text message must be sent to the original SMS Dist list
- The POA Tower Lead, will confirm understanding of Major Incident closure with POL management and POA senior management, and agree next steps

FUJ00080239

7.4 Major Incident Communication Flow Diagram



FUJ00080239

7.5 Major Incident Progress Template

POL agreed template to base MI updates on.

Questions POL need to understand
What is the impact to POL? (Who/What is affected?) *Have we seen calls to the desk/NBSC?* *Can branches trade?*
Which Means? (Expand impact)
What has happened? *Where in the system has a fault occurred?* *Is this in the Fujitsu domain or third party (ie.TTB)?*
When did it occur? *When did we become aware?* *When were POL first notified?*
What are we currently doing to resolve? *Tech Bridge / Who's investigating?* *Who have we escalated to?* *Are third parties involved?* *Have we introduced the IVR? MBS?*
When is it expected to be fixed? *Do we require third party assistance to resolve?*
Why did it occur? *Has it been linked to a change/MSC?*

FUJ00080239

7.6 Escalation Communication Protocol

The primary principle:

Up"
and
"Across

Example:

The Major Incident Manager would escalate up to POA Lead SDM, Problem and Major Incident Management, and across to the Post Office Service Desk.

Major Business Continuity Incidents (MBCI)

For HNG-X the MBCI triggers are listed in:

- HNG-X Support Services Business Continuity Plan (SVM/SDM/PLA/0001)
- HNG-X Services Business Continuity Plan (SVM/SDM/PLA/0002)
- HNG-X Security Business Continuity Plan (SVM/SDM/PLA/0031)
- HNG-X Engineering Service Business Continuity Plan (SVM/SDM/PLA/0030).

These documents should be referred to as appropriate in the event of Major Incident to determine if Business Continuity needs to be invoked.

7.7 Core Major Incident Management Team

The MICM has the task to communicate to Fujitsu Core Major Incident Management team (MIMT) within Resolution Management team (RMT) when an incident meets the criteria of a Major Incident.

- Monday-Friday 08:00 - 18:00 (GMT) - GRO / GRO
- Out of Hours - GRO / Quick Dial no. GRO or GRO

7.8 Corporate Alert

Escalation to Corporate Alerts (in line with the Manage Complaints and Alerts Corporate Business Improvement) is to be approved by POA Business Unit.

FUJ00080239

8 Formal Incident Closure & Post Incident Review

The Post Incident Review is chaired by the Major Incident Manager and follows a set agenda which is distributed with the Post Incident Review meeting invitation, along with the draft copy of the Major Incident Report (if available).

The purpose of a Post Incident Review is:

- To understand the incident that prevented a Service or Services from being delivered.
- To confirm the impact to the business during and after the Incident and agree the number of branches impacted and duration of Major Incident.
- To confirm the end-to-end recovery process and timeline, and identify that all documented processes were followed.
- To analyse the management of the incident and the effectiveness of the governance process.
- To identify corrective actions, including agreed Third Party actions, to:
  - prevent recurrence of the incident
  - minimise future business impact
  - improve the procedure for the management of incidents

Output: To confirm details provided in the draft MIR provided to POL, update with corrective actions and redistribute. To also include any of the following as appropriate

- any activities for a Service Improvement Plan
- any Changes and associated MSC numbers
- any follow up that requires to be progressed via Problem Management
- any improvements to KELS, alerting and /or event management

The agreed impact of the Major Incident must be provided for inclusion in the Counter Availability SLT Figures.

If this review highlights areas where improvements can be made, an agreed Service Improvement Plan will be produced with appropriate actions, owners and timescales. It will also identify any ongoing risks to the service, together with any changes. Service Management will track all actions to resolution. Third party actions will be reviewed at Service Review meetings.

It is important that the number of branches impacted and the duration of the Major Incident is agreed at the Major Incident Review. This information is required to calculate the impact on Branch and Counter Availability and any associated Liquidated Damages (LD) liabilities

FUJ00080239

8.1 Calculating potential LD liability for Major Incidents

Major Incidents which qualify as Failure Events are detailed in the Branch Network Service Description (SVM/SDM/SD0011). A Failure Event is defined in this document as an event or series of connected events which causes one or more Counter Positions to be deemed to be Unavailable due to a Network Wide Failure or a Local Failure. Ongoing failures will be deemed to be part of such a Failure Event until the Failure Event is closed in accordance with the Incident closure and Major Incident Review process as detailed in section 7.0.

For a Failure Event the Incident Closure & Major Incident Review Process will require Post Office and Fujitsu to agree the number of branches and counter positions affected and the duration of the outage (rounded to the nearest 30 minutes as detailed in the Network Wide Rounding Table).

Network Wide Rounding Table

Duration of Incident	Deemed duration for the purposes of LD calculations
30 minutes or less	30 minutes
More than 30 minutes but less than 1 hour	1 hour
1 hour or more but less than 1 hour 30 minutes	1 hour
1 hour 30 minutes or more but less than 2 hours	2 hours
N hours or more but less than N hours 30 minutes	N hours
N hours 30 minutes or more but less than (N+1) hours	(N+1) hours

FUJ00080239

9 Fujitsu Roles and Responsibilities during a Major Incident

This section defines the roles and responsibilities individuals and teams have as part of the Major Incident Escalation Procedure. The following roles will be laminated and available for the MIM to assign during a Major Incident.

9.1 Role of the HSD IMT

The role of the Horizon Service Desk Incident Management Team (HSD IMT) in the event of a Major Incident is as follows:

- Receive and log calls from Post Masters, and communicate the progress of investigations to any Post Masters who call into the desk.
- Escalation of any Call Threshold Breaches to the POA Duty Manager
- Applying and updating IVR, confirming times and details to Major Incident Manager (MIM)
- Send/update service impact details (to include calls offered, abandoned, queuing, trend analysis) to the Major Incident Manager. These details will be fed into the Technical Bridge in real time as requested, whilst details for the overall Major Incident will be provided to the Major Incident Manager post the incident.
- Be responsible for sending communications as provided by the Major Incident Communications Manager for the following:-

  To call and attend all Technical Bridges

  - SMS to SMS Technical Bridge

  To call a Major Incident and provide updates for Major Incident progress, to the following

  - E Mail POL SD
  - Voice POL SD
  - SMS to SMS Internal – POA Internal
  - SMS to SMS TOWER - Senior Management

  NB

  The above communications will be as per instructed by the Major Incident Communications Manager

  ALL should be identical, in order to avoid any misunderstandings.

  This also of course includes notification to POSD and POA Management of the restoration of service.

FUJ00080239

9.2 Role of the Major Incident Manager

Major Incident Manager (MIM). This will by default be either the Day Time Duty Manager or OOH Duty Manager (hours shown in 10.3). However a separate member of the Service Management team may be appointed as the MIM depending on the situation. The primary role of the MIM in a Major Incident is to facilitate the management of the Incident through investigation and diagnosis to resolution, with the aim of making the process as efficient and effective as possible. Upon determining that a Major Incident has been called, a request for a Technical Recovery Manager (TRM) will be made to the appropriate POA Tower lead who will appoint one of his team to be the TRM. The Major Incident Manager acts as the central point for communication and non-technical information flow, allowing the TRM to focus on the technical situation and the resolution of the Incident. The Major Incident Manager is also responsible for creating and maintaining all the associated documentation. For the process to be effective, all updates and information regarding the incident must be fed to the MIM to update the timelines and report.

The Major Incident Manager:

- Calls and chairs the Technical Bridge
- Has responsibility for creating the Major Incident Report, using the template defined in section 10.1 and ensuring that the applicable information is captured.
- Records the Technical Bridge attendees names so they can be documented in the Major Incident Report.
- Identifies Business and Service impact though discussions with the users, the POL Service Desk and the HSD IMT – providing this input into the Tech Bridge.
- Distributes the Technical Bridge actions provided by the TRM (if appropriate).
- In conjunction with the TRM considers if escalation into the Corporate Alert process is desirable and recommends this when required, see section 7.8 above.
- Assists with communication internally within the POA
- Track time lines
- Along with the POA Problem Manager, ensures that the TRM provides regular updates on any longer term corrective actions.
- Following the resolution of the Incident, schedules and chairs the PIR

FUJ00080239

9.3 Role of the Technical Recovery Manager

The primary functions of the Technical Recovery Manager are to co-ordinate and manage the restoration of service, manage the technical teams, and act as the communication point for the technical teams and third parties. The function will also include managing all longer term technical corrective actions, e.g. recommendations for improvements to KELs, eventing and configuration.

The Technical Recovery Manager:

- Manages the technical recovery of the Incident – liaising with SDUs and third parties.
- Provides updates on the recovery, when technicians / representatives of technical teams are unable to attend the Technical Bridge.
- Is the only person to liaise directly with the technical teams, including technical third parties.
- Provides summarised actions from Technical Bridge to the Major Incident Manager, including:
    - Current status including impact and risk
    - Advising on potential workarounds.
    - Planned recovery activities including timelines
    - Root Cause Analysis*, corrective actions, and their corresponding action owners and timelines (where known)

The TRM will be responsible for attending any meetings and providing appropriate root cause analysis and corrective action detail. This will also include managing any longer term technical corrective actions that are documented in the Major Incident Report and will include where appropriate

- Any activities for a Service Improvement Plan
- Any Changes / MSC numbers
- Any Risks
- Any Configuration changes
- Any improvements to KELS, alerting and /or events
- Any associated Peak or TfS calls

- For Root Cause Analysis refer to section 7.0 and Fujitsu Services Business Management Systems Process: Conduct Root Cause Analysis.

FUJ00080239

9.4 Role of the Problem Manager

The Problem Manager ensures that corrective actions / investigations are tracked and completed following the major incident.

Any corrective actions arising from the Major Incident Review will be added to the Major Incident Report and also a Problem Record if appropriate, and tracked with POL through to completion. The updates will be distributed to POL as required, and in the case of a Security Major Incident associated with PCI failures, the POL Security team will also receive a copy of the report.

9.5 Role of the Communications Manager

The Major Incident Communications Manager (MICM) will attend the Technical Bridge and produce each update, where possible trying to ensure that updates are provided on time and following the agreed Major Incident Progress Template. This will reduce any miscommunication and ensure all parties follow process.

- Above all ensuring only one update is circulated
- Will ensure that updates are provided within the agreed times
- Updates will adhere to the agreed Major Incident Progress Template
- Update the master Tfs call with all updates
- Ensure update is provided to IMT to circulate through to POL SD
- Supply update to Service Bridge
- Manages all communication internally within the POA
- Communicate to Fujitsu Core Major Incident Management team
- Manages via IMT, the communication with the POL Service Desk on the progression of the incident

9.6 Role of the SDUs: (Technical Teams /SMC/IMT & Third Parties)

The role is to investigate the Incident, monitor the progress and feed into the Technical Bridge. Also in the event of no pre-determined recovery options, suggest and evaluate potential recovery options to resolve the Incident.

The technical teams should not be contacted by any party other than the Technical Recovery Manager.

The Technical Teams / SMC/ IMT & Third Parties should send an attendee to the Tech Bridge and the associated Major Incident Review meeting. Where attendance on the Tech Bridge is not possible, a suitable alternative resource should attend. If neither is possible then a full update MUST be provided to the TRM to ensure that the Bridge can be updated.

9.7 Role of the Service Delivery Manager owning the affected service

FUJ00080239

- Attends Technical Bridge
- Attends PIR
- Responsible for any further action proposed by the Problem Manager that falls outside the Major Incident closure criteria.
- Responsible for any Service Improvement Plan actions

9.8 Role of the Tower Lead

- Appoint a Technical Recovery Manager
- POA Tower lead will inform within 10 minutes of the start of the service incident the following-
  - POA Delivery Executive
  - POL Senior Service Delivery Managers
- Will coordinate and ensure consistency of response to POL and POA Senior Management via the Service Bridge

FUJ00080239

10 Appendices

10.1 List of Templates

All templates are stored on the central share. : IRRELEVANT under Service Support > Major Incident Management Templates

NAME OF TEMPLATE	DESCRIPTION / NOTES	DISTRIBUTION
Major Incident Report Template	The Major Incident Report contains all the information about a Major Incident. This document is distributed to POL.	POL POA Service Management & Service Operations POA All Tower Leads Fujitsu Support Teams

10.2 Daytime Duty Manager Contact Details

- Steve Bansal – GRO
- Steve Gardiner – GRO
- Tony Wicks – GRO

10.3 Out of Hours Duty Manager Contact Details

- OOH Duty Manager Pager GRO) between the hours:
- 17.30 - 09.00 each day Monday PM to Friday AM
- 17.00 - 09.00 throughout Friday PM and all weekend to Monday AM

Outside these times, please contact the POA Duty Manager

Note: Names and phone numbers are correct at the time of document issue and subject to change. In the event of difficulties refer to the Fujitsu Services Global Address List for the latest details.

FUJ00080239

10.4 POA Service Delivery Contact Details

The Post Office Account service delivery contact details can be found on the Post Office Account Share Point under *Operations* > *BCP* in a folder named *Post Office Account Service Delivery Contact Details*

10.5 Special Situations

10.5.1 Personnel Absence

- In the absence of a POA Tower Lead, an alternative Lead will be appointed.
- Role cards have been produced and will be available to expedite the process

10.5.2 OOH

- The OOH Duty Manager will act as the Major Incident Manager

10.5.3 Duty Manager Change Over

- The Duty Manager at the beginning of the incident will be by default responsible for all MIM communications responsibilities unless a different arrangement is made between the outgoing and incoming Duty Managers