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.

1 **Author & Dept:** Tony Wicks – POA Operations; Aleksandra Zawislak

Internal Distribution: As listed on pages 4 and 5 for

Mandatory Review

Optional Review

Issued for information

External Distribution: For information

Andrew Garner (POL), Gary Blackburn (ATOS)

Security Risk Assessment Confirmed YES

Approval Authorities:

Name	Role	Signature	Date
Steve Bansal	Senior Service Delivery Manager	See Dimensions for record of approval.	

0 Document Control

0.1 Table of Contents

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for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes.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	
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.	
8.1	10-Jun-2014	Amended to replace the HSD function with the Atos Service Desk and replaced IMT references with the MAC team. Also updated to reflect the introduction of Atos as POL's Service Integrator.	
9.0	14-Aug-2014	Implemented minor changes following 8.1 review cycle.	
9.1	22-Jan-2015	Optional Reviewers amended to include Chris Harrison & Shaun Stewart. Section 3.3.5 POLSAP Service Triggers added Section 10.1 amended to refer to the Major Incident Report and Post Incident Review Report templates which are now held in Dimensions.	
10.0	12-Feb-2015	Minor update to section 9.1 and issued for approval.	
10.1	10-Sep-2015	Note added to Section 1.1 General revision to reflect recent organisational changes, the removal of the Engineering service. Created table entry 6.13 and section 8.2 to cover the production and management of multiple versions of the Major Incident Report	
10.2	22-Sep-2015	Minor changes for comments received from informal review and issued for formal review.	
11.0	12-Jan-2016	Section 4.0 updated, table entry 6.12 amended, other minor updates and issued for approval. – This Version was REJECTED in Dimensions.	
11.1	23-Jun-2016	Section 4, Security Major Incidents deleted. Re-aligned cross references to section numbering from 5 onwards	
11.2	19-Jul-2016	Revised to include feedback from Steve Bansal replacing Tower Lead with Senior SDM and/or Service Lead and incorporated changes requested by Bill Membery.	
12.0	19-Jul-2016	Approval version	
12.1	14-Dec-2016	Section 3.3.5 POLSAP Service Triggers modified to reflect 5th October 2016 migration of POLSAP application support to Accenture. Section 7.1 modified to include recommendations to share lessons learnt across Fujitsu, as per the Fujitsu EMEIA Business Management System Major Incident Procedure issued on 28th July 2016.	
12.2	09-Jan-2017	Removed Sandie's name from optional review –appeared twice	
13.0	12-Jan-2017	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks
Mandatory Review	
Role	Name
Senior Service Delivery Manager	Steve Bansal
POA Acceptance Manager	Steve Evans
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andrew Hemingway
POA Business Continuity Manager	Almizan Khan
3 POA Problem Manager	~~Stephen~~Steve Gardiner
POA Lead SDM Online Services	Yannis Symvoulidis
POA Senior Ops Manager HNS	Alex Kemp
POA SDM Major Account Controllers	Sandie Bothick
4, 5 POA ~~SMC~~Operations Manager	~~Catherine Obeng~~Jerry Acton
POA Security Manager	Jason Muir
6 POA Problem & Major Incident Manager	~~Jolene Ngu~~Joe Curtin-Sewell
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	Steve Godfrey

(*) = 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:

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/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Services 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			Manage Major Incidents Procedure	BMS
FJ- BMS- 1-AB1.6			Fujitsu Services Business Management Systems Process: Conduct Root Cause Analysis	BMS
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions
ARC/SEC/ARC/0001			Security Constraints	Dimensions

ISSC-11a			Information Security Incident Management Procedure	ATOS

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

0.6 Abbreviations

Abbreviation	Definition
A+G	Advice & Guidance
BCP	Business Continuity Plan
BMS	Business Management System
7 EMEIA	Europe, Middle East, India and Africa
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEDB	Known Error Database
KEL	Known Error Log
MAC	Major Account Controllers
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
OOH	Out Of Hours
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
SISD	Service Integrator Service Desk (Atos Service Desk)
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

Term	Definition
8 EMEIA Business Management System	The EMEIA Business Management System (EBMS) is the central library for all Policy, Process and associated assets which provides Fujitsu with the responsible way of working that keeps the company, its employees and the services we deliver efficient, effective and compliant
Fujitsu EMEIA	Refers to Fujitsu Services Holdings PLC, Fujitsu Technology Solutions (Holding) BV and their subsidiaries, whether they be incorporated within the EMEIA Region or not, and any other company or organization that is managed by the EVP, Head of EMEIA Region.
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.

1 Introduction

1.1 Owner

The owner of the Major Incident Management process at the local POA level is the Fujitsu POA Senior 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 service integrator and/or the customer
- Demonstrating a professional approach to Atos, the Service Integrator contracted to POL, and Post Office Limited (the customer) and their clients.
- 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'

Note: This procedure is based upon the historical processes agreed between Post Office Limited and the Post Office Account over a period of around fifteen years.

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.

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 MAC Core Hours (Monday – Friday 08:00 – 20:00, Saturday 08:00 – 17:00) and Bank Holidays 0800 – 1400 excluding Christmas Day. The MAC should be the first point of operational contact between Fujitsu and the Atos Service Desk. Outside these hours the Atos Service Desk or Atos OOH Duty Manager should contact the SMC. The SMC are responsible for escalation of incidents to the POA OOH Duty Manager. The POA OOH Duty Manager may initiate communications with the Atos OOH Duty Manger. The SMC operate on a 24 x 7 x 365 basis.

- Any activity detailed in this document which is assigned to the MAC team is handed over to the SMC outside the MAC 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 Atos Service Desk for awareness and monitoring in Atos. This is usually done via the MAC team 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 9.3) to their counterpart in Atos. 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 MAC team (see operational hours above.). 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.

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 incident classification on Post Office Account refer to the POA Incident Enquiry Matrix SVM/SDM/SD/0023.

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.

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 Atos Service Desk in accordance with whichever organisation manages that supplier relationship.

3.3.5 POLSAP Service Triggers

POLSAP services Major Incident Triggers are as follows:

- Business stopped for any Fujitsu controlled reason, e.g. infrastructure failure/outage that would render Post Office unable to process ~~any~~ POLSAP business transactions.
- Outage of key Fujitsu infrastructure which affects the POLSAP services.
- A POLSAP ~~central system~~infrastructure security incident

Whilst the POLSAP/Credence servers are maintained as a part of Fujitsu infrastructure, the cut over point of POLSAP services migrated to Accenture on 5th October 2016 and incidents relating to POLSAP application should be routed to the third party via the ATOS Service Desk. Accenture support would include, among others, the below which were previously solely Fujitsu responsibility:

- A POLSAP local environment failure resulting in Post Office departments being unable to process work, e.g., FSC (POL settling with clients and tracking stock and cash for Post Office Ltd), Supply Chain (Cash Services Business Unit) or Cash Services CMS System (Quotations and Client Management)
- Complete loss of a ~~Fujitsu supported~~ POLSAP application.
- ~~Outage of key infrastructure which affects any of the above POLSAP services.~~A POLSAP application security incident

3.1.6 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
- Either Cardholder Data or Sensitive Authentication Data not being handled as described in the CCD entitled “Security Constraints” (ARC/SEC/ARC/0001).

In the event of a Security Incident, minor or major (which may also include PCI Incidents), the POA Operational Security Manager MUST be informed.

The POA Incident Management procedure SVM/SDM/PRO/0018 Appendix A provides further guidance on security incidents and the contact details for the POA Operational Security Manager is contained in Appendix B.

4 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.)

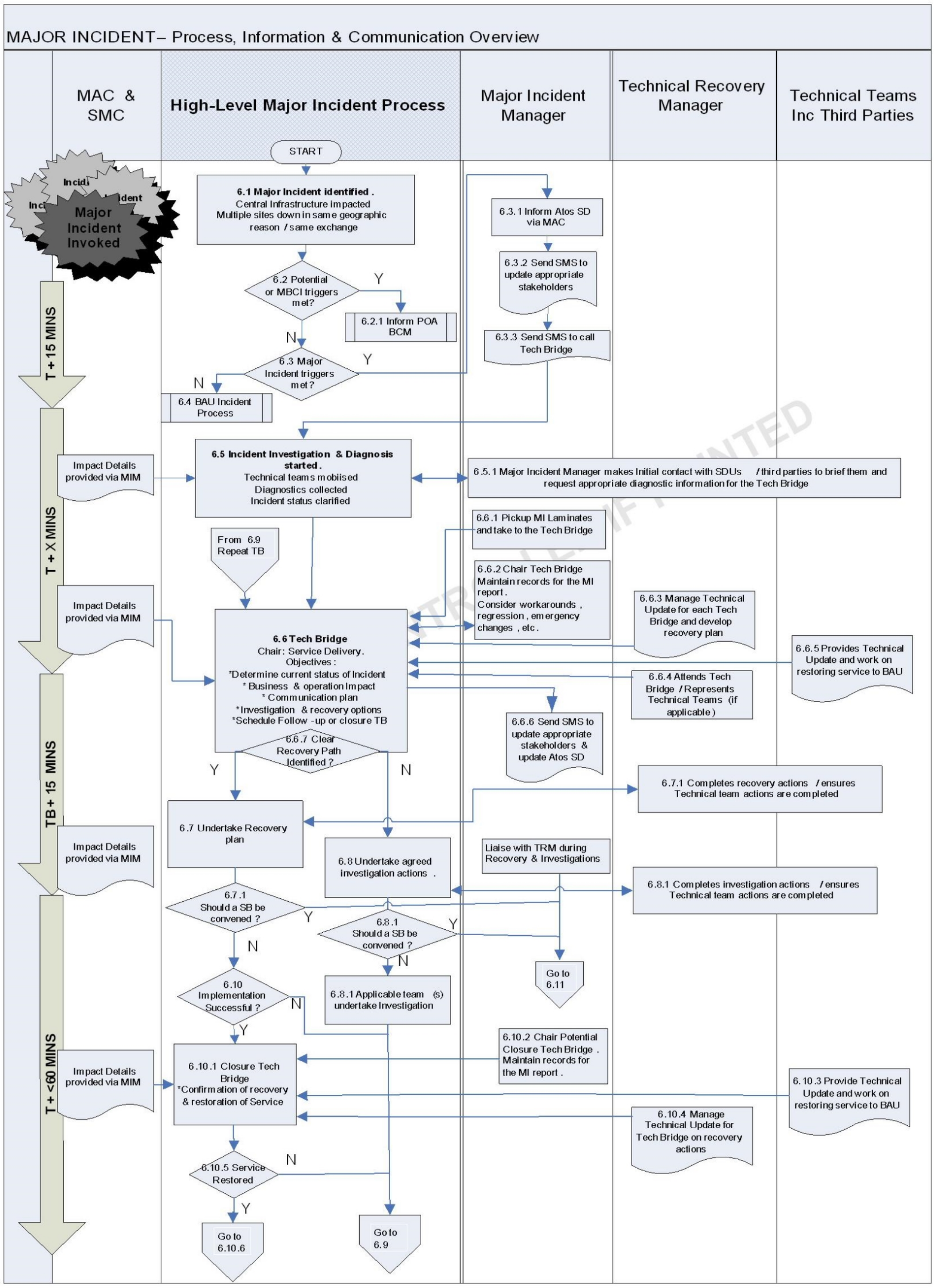
Where the impact of the incident is not immediately obvious, and it is not clear if a Major Incident should be called, escalation and discussion with the POA Operations Management Team should occur, and a collective decision made. If a Major Incident is not called, the incident should be monitored until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

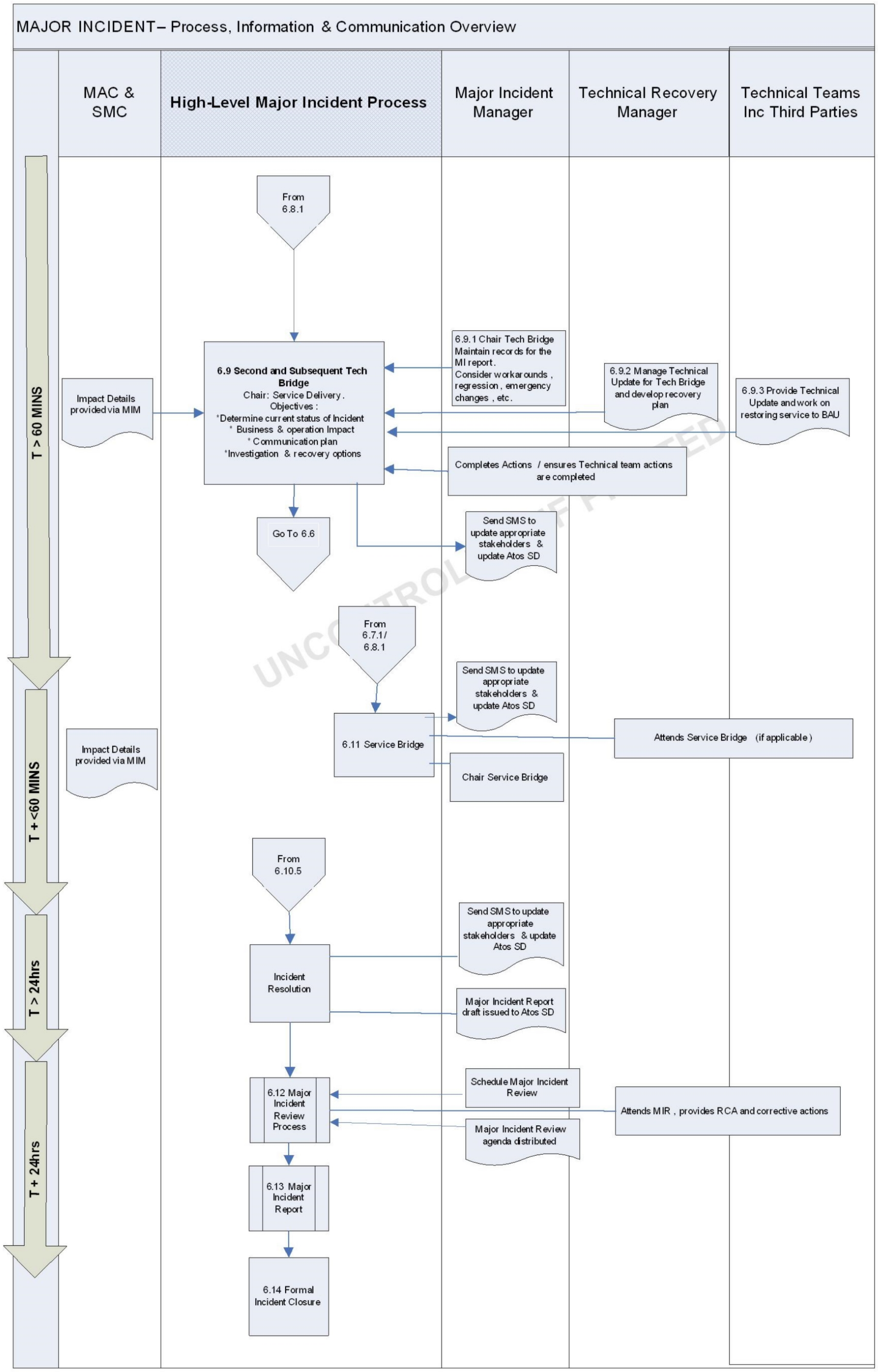
In the event that multiple services are impacted, multiple Major Incident Managers may be appointed by any Service Lead or Senior SDM and will remain in their roles until incident closure.

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

Section 8 of this document specifies the roles and responsibilities during a major incident. The Major Incident Manager, see section 8.2, 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.

5 Process Flow


MAJOR INCIDENT– Process, Information & Communication Overview
MAC & SMC
High-Level Major Incident Process
Major Incident Manager
Technical Recovery Manager
Technical Teams Inc Third Parties
Incident
Incident
Major Incident Invoked
T + 15 MINS
T + X MINS
TB + 15 MINS
T + <60 MINS
START
6.1 Major Incident identified .
Central Infrastructure impacted
Multiple sites down in same geographic reason / same exchange
6.2 Potential or MBCI triggers met?
Y
N
6.2.1 Inform POA BCM
6.3 Major Incident triggers met ?
6.4 BAU Incident Process
6.3.1 Inform Atos SD via MAC
6.3.2 Send SMS to update appropriate stakeholders
6.3.3 Send SMS to call Tech Bridge
Impact Details provided via MIM
6.5 Incident Investigation & Diagnosis started .
Technical teams mobiised
Diagnostics collected
Incident status clarified
6.5.1 Major Incident Manager makes Initial contact with SDUs / third parties to brief them and request appropriate diagnostic information for the Tech Bridge
From 6.9 Repeat TB
6.6.1 Pickup MI Laminates and take to the Tech Bridge
6.6.2 Chair Tech Bridge Maintain records for the MI report .
Consider workarounds , regression , emergency changes , etc .
6.6.3 Manage Technical Update for each Tech Bridge and develop recovery plan
6.6.5 Provides Technical Update and work on restoring service to BAU
6.6.4 Attends Tech Bridge / Represents Technical Teams (if applicable)
6.6 Tech Bridge
Chair: Service Delivery.
Objectives :
*Determine current status of Incident
* Business & operation Impact
* Communication plan
*Investigation & recovery options
*Schedule Follow -up or closure TB
6.6.7 Clear Recovery Path Identified ?
6.6.6 Send SMS to update appropriate stakeholders & update Atos SD
6.7 Undertake Recovery plan
6.7.1 Completes recovery actions / ensures Technical team actions are completed
6.8 Undertake agreed investigation actions .
Liaise with TRM during Recovery & Investigations
6.8.1 Completes investigation actions / ensures Technical team actions are completed
6.7.1 Should a SB be convened ?
6.8.1 Should a SB be convened ?
Go to 6.11
6.10 Implementation Successful ?
6.8.1 Applicable team (s) undertake Investigation
6.10.1 Closure Tech Bridge
*Confirmation of recovery & restoration of Service
6.10.2 Chair Potential Closure Tech Bridge . Maintain records for the MI report .
6.10.3 Provide Technical Update and work on restoring service to BAU
6.10.4 Manage Technical Update for Tech Bridge on recovery actions
6.10.5 Service Restored
Go to 6.10.6
Go to 6.9


MAJOR INCIDENT– Process, Information & Communication Overview
MAC & SMC
High-Level Major Incident Process
Major Incident Manager
Technical Recovery Manager
Technical Teams Inc Third Parties
T > 60 MINS
T + <60 MINS
T > 24hrs
T + 24hrs
From 6.8.1
6.9 Second and Subsequent Tech Bridge
Chair: Service Delivery.
Objectives:
*Determine current status of Incident
* Business & operation Impact
* Communication plan
*Investigation & recovery options
Impact Details provided via MIM
6.9.1 Chair Tech Bridge Maintain records for the MI report.
Consider workarounds, regression, emergency changes, etc.
6.9.2 Manage Technical Update for Tech Bridge and develop recovery plan
6.9.3 Provide Technical Update and work on restoring service to BAU
Completes Actions / ensures Technical team actions are completed
Go To 6.6
Send SMS to update appropriate stakeholders & update Atos SD
From 6.7.1/ 6.8.1
Send SMS to update appropriate stakeholders & update Atos SD
6.11 Service Bridge
Attends Service Bridge (if applicable)
Impact Details provided via MIM
Chair Service Bridge
From 6.10.5
Send SMS to update appropriate stakeholders & update Atos SD
Incident Resolution
Major Incident Report draft issued to Atos SD
6.12 Major Incident Review Process
Schedule Major Incident Review
Attends MIR, provides RCA and corrective actions
Major Incident Review agenda distributed
6.13 Major Incident Report
6.14 Formal Incident Closure

5.1 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 0.5 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 Atos Service Desk will be informed by the MAC 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. (Note, in most cases of an issue impacting branches or POL clients, e.g., unable to contact Data-centre, it is more likely that the Atos Service Desk will initially inform the MAC team of the incident.) In the event of either a potential Major Incident or a Major Incident in its own right,		Major Incident Manager (A)	Potential Major Incident advised. (O)

FUJ00080381

		the POA Major Incident Manager will escalate to the Atos Duty Manager or Atos Live Service Manager and advise accordingly.			
6.3.2		With agreement from the POA SDM for the affected service, or the Duty Manager out of hours, an SMS will be sent to POA Management and Atos Duty Manager alerting to the potential existence of a Major Incident.		POA SDM or POA Duty Manager(A)	SMS sent when 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 Atos 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)	Atos SD 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 pick up the Major Incident Laminates from outside the POA 'Parcel Room' or from the desk of the Senior 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 section9.1 for details of the template. The Tech Bridge agenda which covers: **Roll call, Summary / Overview of Incident, Current Impact, Investigation / Recovery Action, Remedial 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	T + 15	Major Incident Manager (A)	The information required to progress the MI investigation, provide updates 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	Tech Bridge + 15	Major Incident Manager (A)	Provide an SMS update. (O)

		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 Atos Duty Manager or Service Management. 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		Technical Recovery Manager (A)	Co-ordinating and Managing the Recovery process. (O) Advising the MIM to call the MI Closure Tech Bridge. (O)

		Bridge. Go to 6.10.			
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, if one has not already been requested. See 6.11 for Service Bridge details.	>T+ 60	Major Incident Manager (A)	Decision on holding Service Bridge (O)
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, if one has not already been requested. 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 step 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 Tech Bridge	The SDU and Third Parties are to provide updates on the actions taken to restore service and confirm that all actions have been completed and that the affected end service has been restored.		Major Incident Manager (A) SDUs & TPs (R)	Actions 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 Atos 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 Atos Managers are involved in the Service Bridge but it would include **all or some** of the following: • Atos (personnel as instructed by Atos Duty Manager or Live Systems Service Mgr) • POA Service Lead or Senior SDM (Chair Person) • POA Other Service Leads or Senior SDMs • POA Problem and Major Incident Manager • POA Business Continuity Manager • POA Security Manager	Timescale dependant upon impact and nature of incident.	Major Incident Manager (A) Atos Service Manager	Relevant decisions and information from the Service Bridge(s) is to be included in the Major Incident Report. (O)

		• POA SDM owning the affected service • POA Technical Recovery Manager • Third Party Executives (if appropriate) • Appointed working group representatives as appropriate • MAC team 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 1, If the MI occurred on infrastructure outside of POAs control, e.g., Fujitsu Shared Network or Third Party environment then a PIR/RCA should be conducted by the accountable party and a POA PIR may not be needed. Additionally, if during the life of a MI the corrective actions have been identified, e.g., within technical bridge meetings and they are detailed in the MI report the POA Senior Service Delivery Manager may decide that a separate PIR review and report are not necessary. Note 2, 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 7.0 for further details and give consideration to the following: • Lessons learnt		POA Senior SDM, Service Operations (A)	Finalise the Major Incident Report (using the output of the PIR). (O)

		• 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			
6.13	Major Incident Report	Table entry 6.10.5 provided advised on the production of the draft Major Incident Report and first formal version. Section 7.2 of this procedure provides greater detail on the production, management and storing of the Major Incident report		POA Senior SDM	Final formal version of the MIR Report (O)
6.14	Formal Closure	All remedial actions completed both short and long term. Including root cause analysis, and also reviewing/closure with Atos all associated Problem Records, including Atos signing off the Major Incident.		POA Senior 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.

6 Communication

6.1 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 Service 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 which is produced using the MIR Report template SVM/SDM/INR/2693 available from Dimension.

6.2 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. Atos Service Management may also be the initiators of a Service Bridge.

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:

- Atos (Personnel as instructed by Atos Duty Manager or Live Systems Service Manager)
- POA Service Lead or Senior SDM (Chair Person)
- POA other Service Leads or Senior SDMs
- 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
- MAC team 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 Atos 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 Atos). Participants required in the Service Bridge will be contacted via SMS as appropriate.

A POA Service Lead or Senior SDM will send out a text via the MAC team 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** Participant code: **GRO** 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 Service Lead or Senior SDM will initiate the call.

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

6.3 Communication Process Flow

- On suspicion or confirmation of a Major Incident, the MIM will escalate to the Senior SDM for the area, Problem and Major Incident Management SDM, and to the POA Service Leads.

- The MIM will inform the Atos Service Desk, via the MAC team, 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 Atos Live Service Manager

- All updates to the Atos Service Desk are via the MAC team, within agreed timescales controlled by the MICM

- The MICM will issue an SMS text to the POA via the MAC team, alerting of potential issues – including date, time, nature of problems, severity, impact and name

- A POA Service Lead or Senior SDM will inform the following within 10 minutes of start of the service incident
    - POA Delivery Executive
    - POL Senior Service Delivery Managers

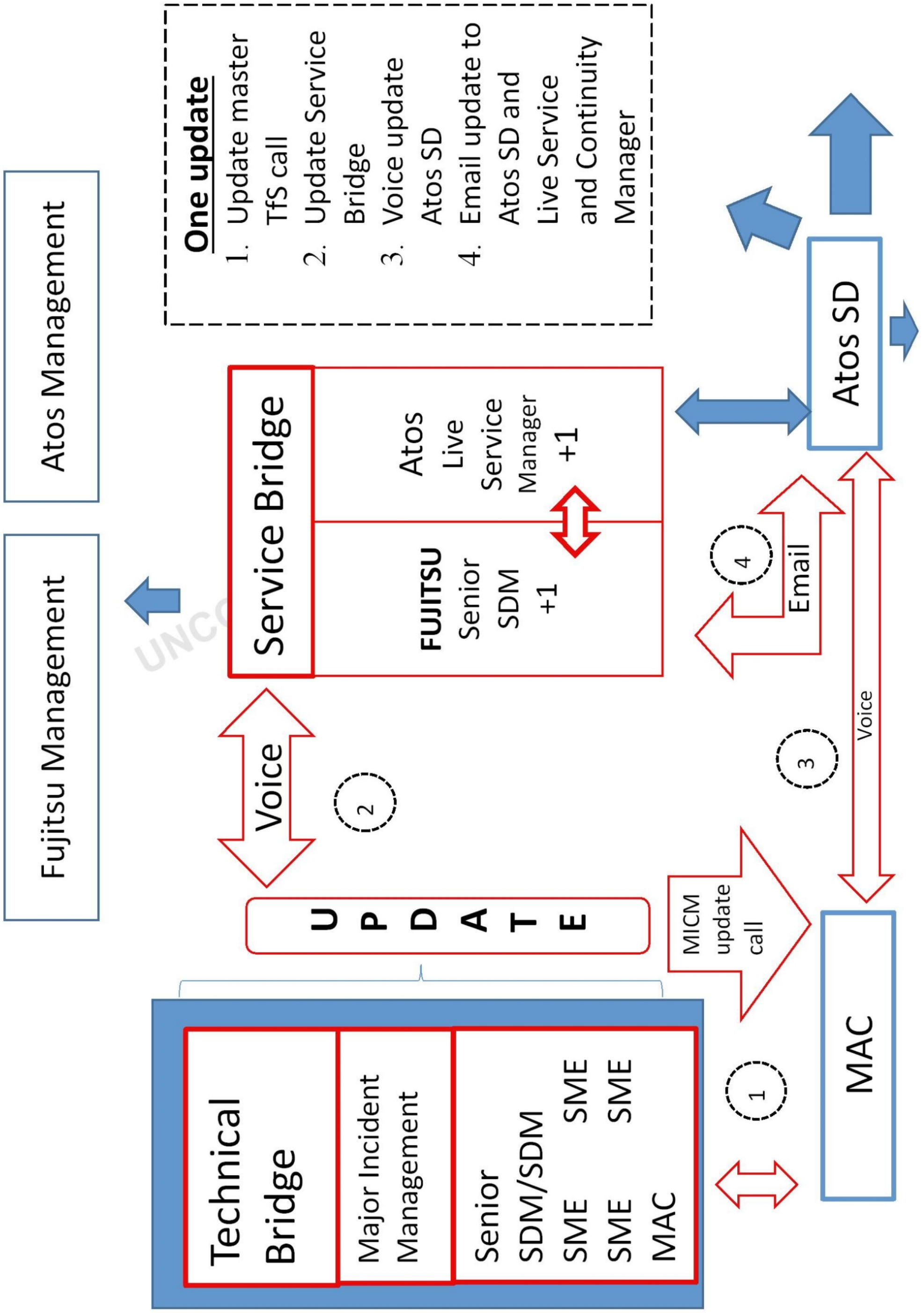
  And will coordinate and ensure consistency of response to Atos and POA Senior Management via The Service Bridge

- 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 Senior SDM, will confirm understanding of Major Incident closure with Atos management and POA senior management, and agree next steps

6.4 Major Incident Communication Flow Diagram



One update

1. Update master TfS call
2. Update Service Bridge
3. Voice update Atos SD
4. Email update to Atos SD and Live Service and Continuity Manager

6.5 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 Atos Service Desk?* *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 Atos first notified?*
What are we currently doing to resolve? *Tech Bridge / Who's investigating?* *Who have we escalated to?* *Are third parties involved?* *Have Atos introduced an IVR or requested an 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?*

6.6 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 Atos 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)

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

6.7 Core Major Incident Management Team

The POA MICM has the task to communicate to Fujitsu Core Major Incident Management team within the Fujitsu Services Resolution Management team when an incident meets the criteria of a Major Incident.

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

6.8 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.

7 Formal Incident Closure & Post Incident Review

7.1 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 template for writing a Post Incident Review Report is stored in Dimension under SVM/SDM/TEM/2531.

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 Atos, 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.

17 Consideration should be given as to whether the improvements can be shared across Fujitsu as lessons learnt, in accordance with Fujitsu EMEIA Business Management System document: Major Incident Procedure (28/07/2016). These are to be documented on the Lessons Learnt portal to help other Accounts to learn from the failures or success of the major incident activities. As stipulated in the document, there may be situations when the lessons cannot be shared due to confidentiality reasons.

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

7.2 The Major Incident Report

The Major Incident Report is produced using the MIR Report template SVM/SDM/INR/2693 available from Dimension.

A first draft of the Major Incident Report is to be produced within 24 hours and on the approval of the POA Senior Service Delivery Manager sent to ATOS Service Management.

The first formal version of the Major Incident Report is to be produced within five working days and on the approval of the POA Senior Service Delivery Manager is sent to ATOS Service Management. Generally this report will be produced after a Post Incident Review is held and the actions for the Major Incident Report identified.

If applicable a Problem Record is to be opened for tracking the corrective actions and managed through the POA Problem Management Process. The formal Major Incident Report version 1.0 is to be attached to the TfS problem record and sent formally for storing in Dimension.

One or more formal versions of the Major Incident Report is to be produced which will also be sent to either ATOS Service or Problem Management, after the approval of the POA Senior Service Delivery Manager, providing feedback on the corrective actions. These major incident reports are also to be attached to the TfS problem record and sent formally for storing within Dimension

7.3 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 6.0.

For a Failure Event the Incident Closure & Major Incident Review Process will require Atos 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

8 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.

8.1 Role of the MAC Team

The role of the Major Account Controllers team in the event of a Major Incident is as follows:

- Receive phone calls and log incidents from Atos Service Desk, and communicate the progress of investigations to the Atos Service Desk.

  Notes:

  1, There is also a HDI interface between Atos SDM12 and Fujitsu TfS systems so incidents and updates may be automatically transferred as well

  2, These incidents are generally considered 'software' incidents as branch engineering incidents are no longer managed by Fujitsu.
- Escalation of any Call Threshold Breaches to the POA Duty Manager
- Confirming times and details to Major Incident Manager (MIM)
- Send/update service impact details from the Atos Service Desk (e.g., trend analysis, which the MAC is dependant upon Atos supplying) 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 send out SMS text messages and attend all Technical Bridges

  - SMS to SMS Technical Bridge

  To inform of new Major Incidents and provide MI updates of progress to the following

  - E Mail Atos Service Desk
  - Voice Atos Service Desk
  - 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 Atos Service Desk and POA Management of the restoration of service.

8.2 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 9.3). 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 Service Lead or Senior SDM 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 section9.1 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 Atos Service Desk and the MAC team – 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 6.8 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

8.3 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 6.0 and Fujitsu Services Business Management Systems Process: Conduct Root Cause Analysis.

8.4 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 Atos 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.

8.5 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 MAC to circulate through to Atos SD
- Supply update to Service Bridge
- Manages all communication internally within the POA
- Communicate to Fujitsu Core Major Incident Management team
- Manages via MAC, the communication with the Atos Service Desk on the progression of the incident

8.6 Role of the SDUs: (Technical Teams /SMC/MAC & 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/ MAC team & 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.

8.7 Role of the Service Delivery Manager owning the affected service

- 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

8.8 Role of the Service Lead/Senior SDM

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

9 Appendices

9.1 List of Templates

All templates are stored in the Document Management Web Service, Dimensions:

IRRELEVANT

The Major Incident Report Template is stored in Dimensions, document reference SVM/SDM/INR/2693.

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 Atos.	See full distribution list in Major Incident Template document SVM/SDM/INR/2693

The Post Incident Review Report template is stored in Dimension under SVM/SDM/TEM/2531.

NAME OF TEMPLATE	DESCRIPTION / NOTES	DISTRIBUTION
Post Incident Report Template	The Post Incident Review Report contains details of the PIR This document is to be treated as an internal Fujitsu document.	Depends upon attendees at the PIR. This document is to be treated as an internal Fujitsu document.

Note: The Major Incident Reports have been formatted to include an ACTIONS section which provides the high level view of the actions identified during the Post Incident Review.

9.2 Daytime Duty Manager Contact Details

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

9.3 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.

9.4 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*

9.5 Special Situations

9.5.1 Personnel Absence

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

9.5.2 OOH

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

9.5.3 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

FUJ00080381

Track Changes

1	Insert	*Matthew Lenton, 21/12/2016 03:23 PM*
2	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
3	Change	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
4	Change	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
5	Change	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
6	Change	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
7	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
8	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
9	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
10	Delete	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
11	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
12	Change	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
13	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
14	Delete	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
15	Delete	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
16	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*
17	Insert	*Zawiślak, Aleksandra, 21/12/2016 03:22 PM*