FUJ00234966

Document Title:	POA Operations Major Incident Procedure
Document Type:	Procedure Definition
Release:	HNG-X
Abstract:	This document details the POA Major incident processes which supplements the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure with the Post Office Limited specific requirements or requests.
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 Matthew Hatch – POA Operations
Internal Distribution:	As listed on pages 4 and 5 for Mandatory Review Optional Review Issued for information
External Distribution:	For information Martin Godbold (POL)
Security Risk Assessment Confirmed	YES

Approval Authorities:

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

FUJ00234966

0 Document Control

0.1 Table of Contents

FUJ00234966

FUJ00234966

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for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes.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	

FUJ00234966

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		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	
13.1	20-Jul-2017	The procedure was checked and updated for CCN1602 (section 3.3.5 amended to remove reference to Credence), CCN1609 (no change) and CCN1614 (section 3.3.1 amended	CCN1602; CCN1609; CCN1614

FUJ00234966

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		to remove reference to the VSAT service). Revised section 0.5.	
13.2	12-Sep-2017	Revised section 9.3, Out of Hours Duty Manager Contact Details.	
14.0	12-Sep-2017	Approval version. Updated link to Dimensions web service, section 9.1.	
14.1	31-May-2018	Major re-write so that the Fujitsu EMEIA Major Incident Procedure is used as the primary process and this document contains customer specific process requirements in managing a major incident. It also contains changes for HDCR changes and amendment in the Acceptance by Document Review, section 0.4. Requested internal Fujitsu Document Review	
14.2	26-Oct-2108	Section 3.3.6, Security Triggers, updated to include breaches of Data Protection Legislation	
15.0	24-Jan-2019	Incorporated changes for comments raised by Steve Bansal and Sandie Bothick. Additionally, further changes made during Author review	

0.3 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks and Matthew Hatch
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
POA Problem Manager	Matthew Hatch
POA Lead SDM Online Services and Risk Manager	Yannis Symvoulidis
POA Senior Ops Manager HNS	Alex Kemp
POA MAC & OBC Manager	Sandie Bothick
POA Operations Manager	Jerry Acton
POA Security Manager	Jason Muir
POA Network Infrastructure SDM	Chris Harrison
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
POA CISO	Steve Godfrey

(*) = Reviewers that returned comments

FUJ00234966

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	3.3.6	Security Triggers
SEC-3095	SEC-3266	SVM/SDM/PRO/0018 section 8.5	Security Major Incidents

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
ARC/SEC/ARC/0001			Security Constraints	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	Dimensions
CS/QMS/001			Customer Service Policy Manual	Dimensions
EMEIA Incident Management Process			EMEIA Incident Management Process	EBMS
EMEIA Major Incident Procedure			EMEIA Major Incident Procedure	EBMS
EMEIA Root Cause Analysis (RCA) Process			EMEIA Root Cause Analysis (RCA) Process	EBMS
ISSC-11a			Information Security Incident Management Procedure	ATOS
PA/PRO/001			Change Control Process	Dimensions
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
SVM/SDM/INR/2693			Major Incident Report Template	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/PRO/0018			POA Operations Incident Management Procedure	Dimensions
SVM/SDM/PRO/0025			POA Problem Management Procedure	Dimensions
SVM/SDM/SD/0011			Branch Network Services Service Description	Dimensions
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions

FUJ00234966

Reference	Version	Date	Title	Source
SVM/SDM/TEM/2531			Post Incident Report Template	Dimensions

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
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
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

FUJ00234966

Abbreviation	Definition
TfS (TfSNow)	Triole for Service – Hosts Incident, Problem and Change databases
TP	Third Party or Third Parties
TRM	Technical Recovery Manager
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

Term	Definition
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.

FUJ00234966

1 Introduction

1.1 Purpose

The purpose of this Post Office Account major incident procedural document is solely to supplement the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure with any Post Office Limited specific requirements or requests.

This document outlines the management guidelines to be used for Major Incidents impacting the live estate in communicating with Atos and Post Office Limited.

1.2 Owner

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

2 Guidelines and Interfacing to Atos

2.1 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

2.2 Interfacing to Atos

- 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. 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 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.
- 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.

FUJ00234966

The communication should include the date, time, name, nature of the incident, priority, 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 Post Office Account defining 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 priority incidents which combine to have a significant business impact.

However not all incidents rated as priority 1 qualify as a Major Incident as the priority 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 priority 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.

FUJ00234966

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.

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)
- 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 POLSAP business transactions.
- Outage of key Fujitsu infrastructure which affects the POLSAP services.
- A POLSAP infrastructure security incident

Whilst the POLSAP 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:

FUJ00234966

- 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 POLSAP application.
- A POLSAP application security incident.

3.3.6 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
- 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) or as required by PCI –DSS.
- Breach of Data Protection Legislation – inclusive of the GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and all other Applicable Law in respect of data protection and data privacy including any applicable guidance or codes of practice that are issued by the Information Commissioner, Working Party 29 and/or the European Data Protection Board (and each of their successors);

In the event of a Security Incident, minor or major (which also include GDPR and 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.

From a corporate perspective the Fujitsu EMEIA SECURITY INCIDENT REPORTING PROCEDURE is to be followed.

3.4 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.

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

FUJ00234966

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.

FUJ00234966

5 Process Flow

As stated in section 1.2 Purpose, this Post Office Account Major Incident Procedural document is solely to supplement the major incident processes defined in the Fujitsu EMEIA Business Management Systems Major Incident Procedure so please refer to the EMEIA procedure and utilise the templates provided within that procedure. These include the Major Incident Report and e-mail templates.

Section 6.4 of this Post Office Account process details the normal Major Incident Communication Flow agreed with Post Office and ATOS the Post Office Limited Service Integrator.

When initiating the Major Incident Report, as required by the Fujitsu EMEIA Business Management Systems Major Incident Procedure, take into consideration the Post Office specific reporting requirements detailed in the Post Office Major Incident Report Requirements contained in section 6.5 below.

6 Communications

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, various Skype functions or voice. The SMS will be sent to the distribution list titled '**Technical Bridge**'. The SMS text or Skype meeting request will be sent to technical experts on the POA account 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.

The Technical Bridge 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 Delivery Unit or Development Leads, who will appoint one of his team to be the TRM.

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

-Recovery / restoration actions (which should normally include the TfSNow Change 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 contained within the Fujitsu EMEIA Business Management Systems Major Incident Procedure

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.

FUJ00234966

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

As a guide the attendance is made up of the following or their designated representative:

- Atos (Personnel as instructed by Atos Duty Manager or Live Systems Service Manager)
- The Senior SDM (Chair Person)
- POA other Service Leads or Senior SDMs
- POA Lead SDM, Problem and Major Incident
- POA Security Manager (If required)
- POA SDM owning the affected service
- Third Party Executives (if appropriate)

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.

The 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, Skype or voice.

The SMS text, email or Skype invitation should state such details as;

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

The chairperson's code is held by the POA Senior SDM and the Problem and Major Incident Managers. The chairperson, normally the 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 the incident, priority 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

FUJ00234966

- The MICM will issue an SMS text to the POA, alerting of potential issues – including date, time, nature of the incident, priority, 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

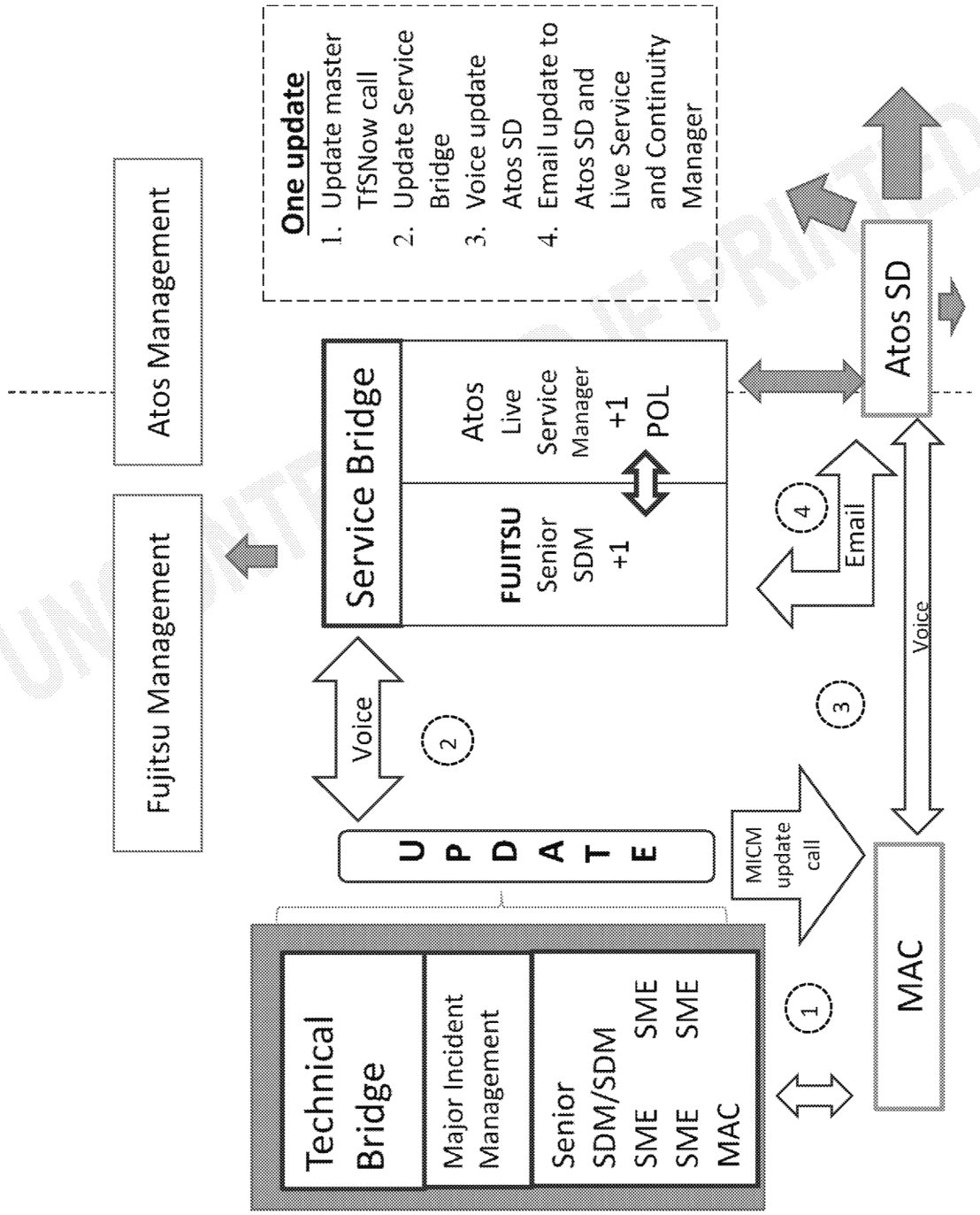
  And will coordinate and ensure consistency of response to Atos and POA Senior Management via The Service Bridge

- Periodic (interval to be determined depending on the nature of the issue but approxiamately 30 minutes as appropriate 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



FUJ00234966

6.5 Post Office Major Incident Report Requirements

POL agreed template to base MI updates on.

Questions POL need to understand
What is the impact to POL? (Who/What is affected?) *Have there been 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 TfSNow Change?*

FUJ00234966

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.

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 (hyperlink below) under SVM/SDM/TEM/2531.

http://europevuk459.europe.fs.fujitsu.com/ccmweb/ProjectHome1.aspx

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 TfSNow Change reference.
- any follow up that requires to be progressed via Problem Management

FUJ00234966

- 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, using the EMEIA SIP template, 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.

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

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 TfSNow 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 TfSNow problem record and sent formally for storing within Dimension

Please use the link below for the EMEIA Standard Major Incident Report

https://emeia.fujitsu.local/emeia/c/P0004/Process_Maps/Major_Incident_Management_Process.pdf

You may need to amend the report template, so it covers the specific requirements of the customer i.e. timeline.

FUJ00234966

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/SD/0011). 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

FUJ00234966

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 TfSNow 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 dependent 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:-

  . If ATOS Incident Management or POL Senior Management send through Technical Bridge requests through to the MAC team and not the POA Duty Manager, to ensure that they are forwarded onto the POA Duty Manager mailbox and the call through if it is short notice.

  To inform of new Major Incidents and provide MI updates of progress to the following
  - E Mail Atos Service Desk
  - Voice Atos Service Desk

  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.

FUJ00234966

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

FUJ00234966

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 / TfSNow Change references
- Any Risks
- Any Configuration changes
- Any improvements to KELS, alerting and /or events
- Any associated Peak or TfSNow calls

* For Root Cause Analysis refer to the Fujitsu EMEIA Conduct Root Cause Analysis Procedure.

FUJ00234966

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 TfSNow 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

FUJ00234966

- 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
  - POL 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 Daytime Duty Manager Contact Details

- Steve Bansal – GRO
- Matthew Hatch – GRO
- Tony Wicks – GRO
- Sandie Bothick – GRO
- Piotr Nagajek - GRO

9.2 Out of Hours Duty Manager Contact Details

The OOH Duty Manager provides cover between 17.30 - 09.00 Monday PM to Thursday AM and 17.00 - 09.00 Friday PM to Monday AM. The OOH Duty Manager can be contacted on the phone number detailed in the *Post Office Account Service Delivery Contact Details* on Share Point (see 9.4 below) or on the date relevant POA OOH Duty Manager rota.

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.

9.3 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*.

FUJ00234966

9.4 Special Situations

9.4.1 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.

9.4.2 OOH

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

9.4.3 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.