FUJ00080189

POA Customer Service Major Incident Process

COMMERCIAL IN CONFIDENCE

Document Title:	POA Customer Service Major Incident Process
Document Type:	Process (PRO)
Release:	Not Applicable
Abstract:	This document describes the Customer Service Major Incident Management Process.
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 FUJITSU (UK & IRELAND) Acceptance Manager.
Author & Dept:	Mike Woolgar – RMG BU CS Service Delivery Manager
Internal Distribution:	Tony Atkinson, David Nicholson, Peter Thompson, Adam Parker, Mike Woolgar, Ian Venables, James Davidson, Andy Gibson, Steve Parker, Dave Jackson, Mike Stewart, Nick Crow, Neneh Lowther, Dave Wilcox, Ian Mills ,Tom Lillywhite Michael Jacklin, Sarah Hill, Leighton Machin, Karen Harrod, Sandie Bothick, Susan Appleby-Robbins, Adrienne Thompson, Claire Drake, Bill Membury, Vince Cochrane, Pat Lywood, Saha Saptarshi, Steve Bansal, Tony Atkinson, Saheed Salawu, John Hill
External Distribution:	Dave Hulbert (POL), Mark Weaver (POL), Gary Blackburn (POL) Alan Simpson(POL)
Security Risk Assessment Confirmed	YES

Approval Authorities:

Name	Role	Signature	Date
Tony Atkinson	RMG BU Head Of Service Operations	See Dimensions for record	

FUJ00080189

0 Document Control

0.1 Table of Contents

FUJ00080189

FUJ00080189

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for Acceptance by Document Review by Fiona Woolfenden including the removal of references to CS/PRD/074 which has been Withdrawn and replaced by SVM/SD/PRO/0018 and other tidying up changes.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

0.3 Review Details

Review Comments by :	
Review Comments to :	Mike Woolgar, Adam Parker & RMGADocumentManagement@ GRO

Mandatory Review	
Role	Name
RMG BU Head of Service Operations	Tony Atkinson
RMG BU Service Operations Lead SDM	Saheed Salawu
Optional Review	

FUJ00080189

Role	Name
RMG BU Business Continuity Manager	Adam Parker
RMG BU Service Delivery Manager Engineering	Susan Appleby-Robbins
RMG BU Service Delivery Manager On-Line Services	Mike Stewart
RMG BU System Support Centre Manager	Pete Thompson
FUJITSU HSD Operations Manager	Michael Jacklin
FUJITSU SMC Manager	Saha Saptarshi
RMG BU Reconcilliations	Claire Drake
RMG BU HSD SDM	Sandie Bothick
FUJITSU Acceptance Manager	David Cooke
Issued for Information – Please restrict this distribution list to a minimum	
Position/Role	Name
RMG BU Service Delivery Manager: Networks	Ian Mills
RMG BU CISO	Tom Lillywhite
Unix Team Leader	Andy Gibson
NT Team Leader	Adrienne Thompson
Network Manager	Dave Jackson
DC Operations Manager	John Hill

(*) = Reviewers that returned comments

0.4 Acceptance by Document Review

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

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			RMGA/POL Interface Agreement for the Problem Management Interface	PVCS
CS/PRD/021			RMGA Problem Management Process	PVCS

FUJ00080189

CS/PRO/110			RMGA Problem Management Database Procedures	PVCS
PA/PRO/001			Change Control Process	PVCS
CS/QMS/001			Customer Service Policy Manual	PVCS
SVM/SDM/SD/0001			Service Desk – Service Description	Dimensions
CS/PLA/015			Horizon Systems Service Desk and Business Continuity Plan	PVCS
SVM/SDM/PLA/0001			HNG-X Support Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0002			HNG-X Services Business Continuity Plan	Dimensions
SVM/SDM/PLA/0030			HNG-X Engineering Service Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			HNG-X Security Business Continuity Plan	Dimensions
SVM/SDM/SD/0011			Branch Network Services Service Description	Dimensions
SVM/SDM/PRO/0018			CS Incident Management Process	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
HSD	Horizon Service Desk
IMT	Incident Management Team
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEDB	Known Error Database
KEL	Known Error Log
MBCI	Major Business Continuity Incident
MIM	Major Incident Manager
MIR	Major Incident Report
MSU	Management Support Unit
OCP	Operational Change Proposal
PO	Post Office
POL	Post Office Limited
RFC	Request For Change
RMG BU	Royal Mail Group Business Unit

FUJ00080189

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, Release Management or Security teams.
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
TB	Technical Bridge
TRM	Technical Recovery Manager
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

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

0.8 Changes Expected

Changes

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.

FUJ00080189

1 Introduction

1.1 Process Owner

The owner of this process is the RMG BU Lead SDM, Service Operations.

1.2 Process Objective

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

- Improvements of communication channels.
- Clarify the need to communicate awareness of potential incidents
- Improved accuracy of reporting against status of incident
- Allowing technical teams the right amount of time to diagnose and impact an incident
- Avoid unnecessary alerting of the customer
- Demonstrate to the Post Office a more professional approach
- Provision of clear defined roles and responsibilities
- Defined reporting/update timelines through duration of a major incident.
- Improved governance
- Assessing which incidents are major and which are 'Business as Usual'

1.3 Process Rationale

This document outlines the communication and management process and guidelines to be followed in relation to Major Incidents impacting the live estate.

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

The aim of the document is to provide a pre-defined process on which future major incident communication and management will follow and that any parties involved in that process provide updates /receive updates at defined intervals from inception to closure of any major service impacts.

FUJ00080189

2 Mandatory Guidelines

Whilst 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) Avoid unnecessary alerting of the customer

c) Assessing which incidents are major

The following guidelines should be adhered to.

- During HSD IMT Core Hours (Monday – Friday 08:00 – 18:00 and Saturday 08:00 – 14:00) HSD IMT should be the first point of contact for operational contact between Fujitsu and the end user. Outside these hours SMC acts as the first point of contact.
- Any activity detailed in this document which is assigned to the HSD IMT is handed over to SMC outside the HSD IMT Core Hours.
- The relevant technical teams who are monitoring and aware of a potential major incident must page/call the appropriate Major Incident Manager (Duty Manager out of hours) as ***soon as possible***, rather than wait This is not limited to major incidents alone, but must be delivered wherever a state other than Business as Usual has been detected. The Major Incident Manager must in turn communicate the potential incident, to POL SD for awareness and monitoring in POL. This is usually done via the HSD IMT in hours.
- The Major Incident Manager (or Duty Manager out of hours) is responsible for communicating both *up* the Fujitsu Organisation and *across* (see appendix 10.3) to their counterpart in POL. Where this is impractical (i.e. leave, out of hours, unavailable), the initiative should be taken to jump up the organisation. The important fact 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 owner for contact.
- The Major Incident Manager (Duty Manager OOH) should also initiate communication using SMS via HSD IMT, 08.00 to 18.00 Monday to Friday, and Saturday 08.00 to 14.00. Outside of these hours, SMS should be via SMC.

FUJ00080189

3 Definition of a Major Incident

3.1 Incident Classification

As a general rule a Major Incident will always be an incident rated as severity level A (critical) in the RMG BU Customer Service Incident Management Process Details document (SVM/SDM/PRO/0018) version 2.0, or a series of connected lower severity rated Incidents which combine to have a significant business impact. However not all incidents rated at severity level A qualify. This is because the severity levels do not necessarily translate to the global business impact on POL's business. For example a single counter post office which is unable to transact, regardless of its business volumes is rated as a Severity A.

For simplicity, Incidents are classified into three impact levels: High, Medium and Low.

High – An Incident that has occurred with a significant and potentially prolonged adverse impact on POL business. Typically these Incidents will initially require a significant amount of reactive management before they can be controlled and resolved.

Medium – An Incident that has the potential to cause significant impact to POL business but can be controlled and mitigated against through effective management.

Low – An Incident that requires business attention but if managed effectively will not have significant impact on POL business.

3.2 Influencing Factors in calling Major Incident

It is important that a major incident is defined 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. The following parameters will also feed into the consideration of whether a major incident exists, as follows:

- 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 – eg Christmas / Easter / End of month/quarter DVLA
- 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 criteria below could trigger a major incident, however as detailed in 3.2, the influencing factors must be considered. As such the list below can never be exhaustive, whilst if an incident occurs which is not detailed, this should not be precluded from being a major incident.

FUJ00080189

3.3.1 Network Triggers

Network Major Incident triggers are as follows:

- Complete or significant outage of Central network
- Complete or significant outage of BT network
- Complete or significant outage of VSAT sites

3.3.2 Infrastructure Components Triggers

Infrastructure component Major Incident Triggers are as follows:

- Total loss of environments providing individual on-line 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
- Breach of security

3.3.4 On-Line Services Triggers

On-Line services Major Incident Triggers are as follows:

- On-line service unavailable within Data centre (not counter level)
- Number of Branches not able to provide on-line services – as defined by POL
- 3rd party provided service failure – Link, Fujitsu Group

3.3.5 Security Triggers

Security major incident triggers are as follows:

- Actual or suspected attacks on the Fujitsu Services RMG BU Network or Information System.
- Theft of IT equipment / property, including software

In the event of a Security Major Incident (which may also include PCI Incidents), the security incident management process as detailed in

SVM/SDM/PRO/0018 Appendix A must also be followed by the security SDM.

FUJ00080189

SVM/SDM/PLA/0031 HNG-X Security Business Continuity Plan defines the actions to be taken if security violations are identified. This must also be followed by the SDM owning the service.

FUJ00080189

4 Calling the Major Incident

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

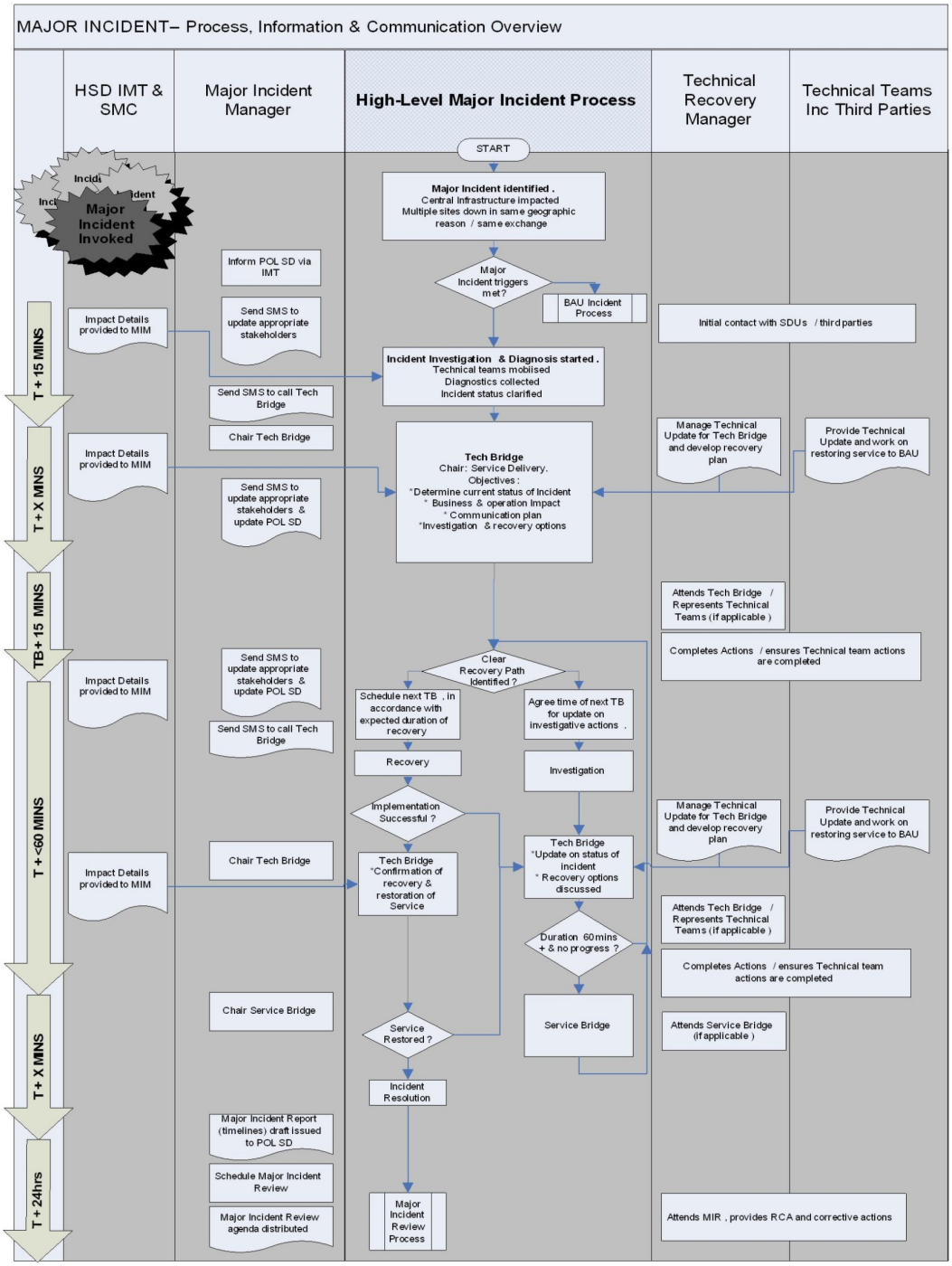
Where the impact of the incident is not immediately obvious, and it is not clear if Major Incident should be called, escalation and discussion with the RMG BU Lead SDM, Service Operations, RMG BU Head of Service Operations or RMG BU Service Director should occur, and a collective decision made. If Major Incident is not called, the incident should be monitored until closure, to ensure that the impact does not increase to Major Incident.

In the event that multiple Services are impacted, multiple Major Incident Managers will be appointed by RMG BU Lead SDM, Service Operations, RMG BU Head of Service Operations or RMG BU Service Director, who will remain in this role until incident closure.

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

FUJ00080189

5 Process Flow



FUJ00080189

5.1 Process Description (Any reference below made to T, = Time of incident occurring. Hence T+3 = Time Incident Occurred plus 3 minutes).

Box Title	Description	Key timescales	Action owner
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		
Major Incident Triggers Met?	An initial impact assessment of the incident is undertaken by members of the RMG BU Service Team taking into account impact on: Live Service, Financial Integrity, Business Image The incident is profiled as a Major Incident as outlined within this document, including consideration of all influencing factors, time, geographical coverage, business impact, security, public perception, duration and relevant business initiatives coinciding at POL and decision taken to call Major Incident. The Major Incident Manager will consult with the Business Continuity Plans (Ch 10.6) to identify if potential MBCI or MBCI triggers have been met and inform RMG BU Business Continuity Manager if appropriate. POL SD will be informed by the Major Incident Manager of the incident & the incident will also be escalated to Service Delivery / Service Support team managers, if this has not already occurred. With agreement from RMG BU Service Delivery Manager, or Duty Manager out of hours, SMS will be sent to RMG BU and POL Management alerting to the potential existence of a Major	T+3 All timescales quoted within this document as viewed as maximum, to be improved upon wherever possible T+5	Major Incident Manager Major Incident Manager HSD IMT (in hours) SMC (out of hours)

FUJ00080189

	Incident.		
BAU Incident Process	If Major Incident is not declared then the BAU Incident process is followed – POL SD will be informed that there is no MI & a closure SMS sent. The 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 Major Incident, move to box "Incident Investigation and Diagnosis started".		
Incident Investigation & Diagnosis	Relevant internal SDUs / Third Parties contacted to initiate investigation & diagnosis. Major Incident Report opened Tech Bridge scheduled & agenda distributed.	T+ 5	Major Incident Manager Major Incident Manager
Tech Bridge	The Tech Bridge is chaired by the Major Incident Manager with assistance from the Technical Recovery Manager. The Tech Bridge is SERVICE FOCUSSED. The Tech Bridge aims : • To discuss & agree the recovery investigation & resolution of Major Incidents • To provide a forum for up-to-date progress reports • To aid communication, and the creation of Technical Bridge Minutes which are distributed to all involved parties and RMG BU & POL Management. This ensures that Major Incident progress is known by all. • To collate information for inclusion on the Service Portal. Attendees at the Tech Bridge include, but are not limited to, RMG BU Service Management, SDU, Third Parties, POL, CS Security & POL Security Managers	T + 15	Major Incident Manager

FUJ00080189

	The Tech Bridge follows a set agenda which covers: **Roll call, Summary of Incident, Incident Overview, Current Impact, Current Investigation / Recovery Action, Remedial Actions, Actions to carry forward to Major Incident Review** The agenda template is stored on **IRRELEVANT** Following the Tech Bridge, a further SMS will be sent, providing an update on the Incident If the outcome of the Tech Bridge is that the Incident is determined Business As Usual (low) then an SMS communication will be sent stating that the Incident is not a Major Incident. From this point forward, SMS communication, timing and delivery requests, becomes the responsibility of the Major Incident Manager. 30-minute updates should be the norm The Major Incident Manager will also distribute minutes following the conference call. TRM will provide summary minutes to the MIM who will distribute the minutes. At the time agreed at the first Tech Bridge, the subsequent Tech Bridges are held. 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	Tech Bridge + 15	

FUJ00080189

Clear recovery path identified	If during the conference call a clear recovery path is identified, this should be discussed and agreed on the call. Following agreement the recovery should be implemented. If there is no clear recovery path, further investigation will be undertaken.		
Recovery / Investigation	The Technical Recovery Manager will liaise with the SDUs and /or third parties during the investigation / recovery. Where appropriate a Technical Bridge will be called for a technical discussion of the Major Incident.	T + x	Technical Recovery Manager
Tech Bridge 1+		T + x	Major Incident Manager
Service Bridge	The nature of the incident determines which RMG BU Service Team members and POL Managers are involved in the Service Bridge but it would include all or some of the following: • POL • Major Incident Manager (Service Bridge Chairman) • Technical Recovery Manager (if appropriate) • RMG BU Service Director • RMG BU Head of Service Operations • RMG BU Lead SDM, Service Operations • 3rd party Executives (if appropriate) • Appointed working group representatives as appropriate The purpose of the Service Bridge is to: • Provide appropriate direction on Incident resolution	Timescale dependant on impact and nature of incident.	Major Incident Manager POL Service Manager

FUJ00080189

	• Provide added impetus to restoration of service ASAP • Define communication intervals to Key Stakeholders • Provide focused Incident Management in line with the impact and severity of the Incident.		
Incident Resolution	Once the incident is deemed to be resolved, final Tech Bridge is held to agree & confirm resolution of incident. Major Incident Review date to be set at the final Tech Bridge. SMS communication sent confirming resolution of incident. Draft Major Incident Report distributed within 24hrs of resolution of Major Incident.		Major Incident Manager
Major Incident Review & formal Incident Closure	Formal Closure of the Major Incident & a review of the Incident including consideration of: • Lessons learnt • Incident definition • What went well • Timeline • Changes required to infrastructure • A review of the Major Incident Communication Process • Root Cause Analysis * if known at this point • Business impact • Action plan • Service Improvement Plan update		RMG BU Lead SDM, Service Operations

FUJ00080189

6 Conference Calls

6.1 Tech Bridge

Dial in details: [redacted] Participant code: [redacted]

This is a technical conference for experts to discuss and analyse the incident enabling an appropriate action plan to be formulated to restore the service to POL without delay. The Technical Conference Call will baseline the anticipated response, covering resolution, time and resources required.

The Technical Conference Call will be incepted as required by the Major Incident Manager.

Invitations to the Tech Bridge will be via SMS, email or voice. The dial in details will be provided at the same time as the meeting invitation.

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

Each Tech 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.

Following each Tech Bridge, a set of minutes will be published, which will subsequently form part of the Major Incident Report stored on [redacted] under Service Support > Major Incident Reports.

6.2 Service Bridge

Dial in details: [redacted] Participant code: [redacted]

This is a Service Focussed call for Service Management (including technical recovery manager) and POL to discuss the service impact of the Major Incident and to receive updates on progress of the Incident.

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

Attendance will be mandatory from the following or their designated representative:

- RMG BU Service Director
- RMG BU Head of Service Operations
- RMG BU Business Continuity Manager
- RMG BU Service Delivery Manager / Owner (Business line specific)
- POL Head of Technical Services
- POL Service Delivery Manager
- POL Business Continuity Manager
- 3rd Party Account/Service Delivery Manager
- RMG Security Manager (If MI is a PCI or Major Security Incident)
- POL Security Incident Manager (If MI is a PCI or Major Security incident)

FUJ00080189

Actions within the Service Bridge include:

- Agreement of Containment Plan
- Documentation of all agreed actions with owners, and timescales
- Consistent management of the major incident across all involved locations
- Management of potential / MBCIs within POL & RMG BU
- Co-ordinate meeting times and locations

In the event of a major incident requiring a Service Bridge to be incepted, it is envisaged that this will be in place at T+60. Participants required in the Service Bridge will be contacted via SMS as appropriate.

The Major Incident Manager will call and chair a Service Bridge. The chair person's code is held by the RMG BU Service Director, RMG BU Head of Service Operations, RMG BU Lead SDM, Service Operations. The Chairman will enter the call prior to the attendance of other callers and enter a designated PIN, allowing direct entry for subsequent callers.

The TRM will be responsible for attending any meetings and providing appropriate root cause analysis and corrective action detail

The Major Incident Review is chaired by the Major Incident Manager and follows a set agenda, which should be distributed with the Major Incident Review meeting invite, along with the draft copy of the Major Incident Report.

FUJ00080189

7 Formal Incident Closure & Major Incident Review

The purpose of a Major Incident Review is:

1. To understand the Incident that prevented a Service or Services from being delivered.
2. To confirm impact to the business, during and after the Incident and agree number of branches impacted and duration of Major Incident.
3. To confirm the end-to-end recovery process & timeline and identify that all documented processes were followed.
4. To analyse the management of the Incident & the effectiveness of the governance process.
5. To identify corrective actions to:
   i. prevent recurrence of Incident
   ii. minimise future business impact
   iii. improve management of Incidents
6. To formally close the Major Incident

Output: To confirm details provided in the draft MIR provided to POL, update with corrective actions and redistribute. The agreed impact of Major Incident must be sent to Branch Network Service Delivery Manager 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. Service Management will track all actions to resolution. Third party actions will be reviewed at Service Review meetings.

The Agenda for the Major Incident Review is stored on:
IRRELEVANT under Service Support > Major Incident Management Templates

It is critical that the number of branches impacted and the duration of the Major Incident is agreed at the Major Incident Review and this agreement must come from POL. If for some reason POL is not present at the Major Incident Review meeting, a separate conversation must take place. This information is required because Major Incidents affect Counter Availability and Liquidated Damages (LDs) are paid on Counter Availability as detailed in 7.1 below.

7.1 Calculating Liquidated Damages payable on Major Incidents.

Liquidated damages are payable on Major Incidents which qualify as Failure Events as detailed in the Branch Network Service Description (SVM/SDM/SD0011). 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 Failure Event until the Failure Event is closed in accordance with the Incident closure and Major Incident Review process as detailed in section 7.0.

For a Failure Event the Incident Closure & Major Incident Review Process will require Post Office and Fujitsu Services to agree the number of Branches and Counter Positions affected and the duration of the outage;

The duration of the Incident must be agreed with Post Office & rounded to the nearest 30 minutes as detailed in the Network Wide Rounding Table below

Network Wide Rounding Table

Duration of Incident	Deemed duration for the purposes of LD calculations

FUJ00080189

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

FUJ00080189

8 Fujitsu Services Roles and Responsibilities During a Major Incident

This section defines the roles and responsibilities individuals and teams have with regard to the Major Incident Escalation Process.

8.1 Role of the HSD IMT

The role of the Horizon Service Desk Incident Management Team (HSD IMT) in the event of a Major Incident is two-fold

- Receive & log calls from the Post Masters, and communicate the progress of investigations to any PMs who call into the desk.
- The HSD IMT should also send impact details (to include calls offered, abandoned, queuing) to the Major Incident Manager, who is managing the Incident. This template should be completed every 15 mins from the point of declaring Major Incident, until the Major Incident Manager asks for this to cease.

8.2 Role of the Major Incident Manager

The primary role of the Major Incident Manager 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 & effective as possible. The Major Incident Manager acts as the central point for communication and non-technical information flow, allowing the Recovery Manager to focus on the technical & the resolution of the Incident. The Major Incident Manager is also responsible for creating and maintaining all the associated documentation.

The Major Incident Manager:

- Has responsibility for creating the Major Incident Report
- Manages the communication, internally within RMG BU.
- Communicates progress of Incident with POL SD
- Identifies Business & Service impact, though discussions with the users, POL SD & HSD IMT – providing this input into the Tech Bridge.
- Calls & chairs the Tech Bridge
- Distributes the Tech Bridge minutes provided by TRM (if appropriate).
- Liaises with SSC to update the Service Portal

Following resolution of the Incident the Major Incident Manager schedules and chairs the Major Incident Review and creates the Major Incident Report Document.

FUJ00080189

8.3 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 corrective actions log and tracked through to completion. The updates will be distributed to POL as required, and in the case of a Security Major Incident associated with PCI failures, then the POL Security team will receive a copy of the report.

8.4 Role of the Technical Recovery Manager

The primary functions of the Technical Recovery Manager is to act as Recovery Manager co-ordinating and managing the restoration of Service, managing the technical teams and acting as the communication point for the technical teams and 3rd parties.

The Technical Recovery Manager:

- Manages the technical recovery of the Incident – liaising with SDUs & Third Parties.
- Provides updates on the recovery, when technicians / representatives of technical teams are unable to attend the Tech Bridge.
- Provides the MIM with tech bridge summary minutes
- Is the only person to liaise directly with the technical teams, including technical third parties.
- Provides summarised minutes from Tech Bridge to MIM including:
    - Current status including impact and risk
    - 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.

FUJ00080189

8.5 Role of the SDUs: Technical Teams / Third Parties

The role is to investigate the Incident, and in the event of no pre-determined recovery options, suggest and evaluation of 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 / 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 full update MUST be provided to the TRM to ensure that the Bridge can be updated.

8.6 Role of the Service Delivery Manager Who Owns the Affected Service

- Attends Post MI review
- Responsible for any further action proposed by the problem manager that falls outside of the MI closure criteria.

FUJ00080189

9 Post Office / Fujitsu Services Interfaces

The Post Office / Fujitsu Services interfaces are all detailed in the Process Description, section 5.1, however for ease the interfaces have been extracted into the table below.

POL SD & POL management stakeholders updated – updated within 15 minutes of the major incident and after this as per agreed timeline.

Draft MIR (timelines) provided – provided by the Major Incident Manager within one working day

MIR (timelines, root cause analysis, corrective actions) provided - provided by the Major Incident Manager within one working week

Service Bridge invitation – when MI has been unresolved for greater than an hour or it is deemed appropriate.

As detailed under Appendix 10.3, escalation of the Major Incident will also occur; this activity running concurrently to the interfaces detailed above.

FUJ00080189

10 Appendices

10.1 List of Templates

All templates are stored on the central share. :

IRRELEVANT

NAME OF TEMPLATE	DESCRIPTION / NOTES	DISTRIBUTION
Major Incident Report Template	The Major Incident Report contains all the information about a Major Incident. This document is distributed to POL.	POL RMG BU Service Support & Service Delivery RMG BU Head of Service Operations RMG BU Service Director RMG Core Service Support Teams
Major Incident Review Minutes	Standard format for Major Incident Review minutes. Ensures that information is collected in correct format for inclusion in other reports / to be taken to Service Review.	Attendees of MIR RMG BU Service Support & Service Delivery RMG BU Head of Service Operations RMG BU Service Director RMG Core Service Support Teams

FUJ00080189

10.2 Major Incident Manager Contact Details

- Mike Stewart GRO
- Mike Woolga GRO

10.3 Out of Hours Duty Manager Contact Details

OOH Duty Manager Pager GRO is to be used between the hours:

17.30 - 09.00 Monday PM to Thursday AM

17.00 - 09.00 Friday PM to Monday AM

Outside of these times, please contact the Major Incident Manager

10.4 Service Delivery Managers Contact Details

AREA OF RESPONSIBILITY	EXAMPLE INCIDENTS	ESCALATION TO:	CONTACT DETAILS	BACK UP
Infrastructure issues. NT / UNIX / Data Centres All network issues	Network Incidents Data centre issues Storage Incidents NT /UNIX Incidents	**Ian Mills/Claire Drake**	GRO GRO	Tony Atkinson
Banking and Online Services (Inc: DVLA, Debit Card, EPAY)	Online Service outages	**Mike Stewart** 1st point of contact	Pager GRO Mobile GRO	Tony Atkinson GRO 3rd point of contact
Banking and Online Services (Inc: DVLA, Debit Card, EPAY)	Online Service outages	**Mike Woolgar** 2nd point of contact	Pager GRO Mobile GRO	Tony Atkinson GRO 3rd point of contact
Reference data escalations	New product not functioning	**Dave Wilcox**	GRO	Kevin Mckeown GRO
Engineering	Major issue with engineering service	**Susie Appleby-Robbins**	GRO	Nominated by Leighton Machin GRO

FUJ00080189

OBC Escalations	OBC job going wrong/ press involved /unhappy postmaster	**Ian Venables**	GRO	Chris Bourne GRO
Major software problem	Major software problem	**Steve Parker**		John Simpkins GRO
HSD/ PostShops	Major TFS call logging issues. Major PostShop outage	**Sandie Bothick**		Sarah Bull GRO
Security	Security Issues Virus Alerts	**Tom Lillywhite**		Bill Membury GRO
Release Management / Service Introduction	Issues caused by Releases	**Sarah Bull**		Tony Atkinson GRO
SMC	Monitoring/ eventing of data centre environment	**Saheed Salawu**		Tony Atkinson GRO

FUJ00080189

10.5 Escalation Communication Protocol

The primary principle:

Up"

and

"Across

Example:

MIM would escalate up to RMG BU Lead SDM, Service Operations and across to PO SD.

10.6 Major Business Continuity Incidents (MBCI)

For Horizon the MBCI triggers are listed in:

- Horizon Services Business Continuity Plan (CS/PLA/079)
- Horizon Support Services Business Continuity Plan (CS/PLA/080)
- Horizon Service Desk Business Continuity Plan (CS/PLA/015).

For HNG-X the MBCI triggers are listed in:

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

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

10.7 Security Major Incidents

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

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

FUJ00080189

10.8 Roles

- MIM – Major Incident manager. This will by default either the day time or OOH duty manager. A separate member of the Service management team can be appointed as the MIM depending on the situation. The MIM will handle all communications to IMT and keep track of time lines. The MIM is also responsible for sending SMS messages but this can be delegated. The MIM will be assisted by a Problem Manager who will be responsible for taking notes and coordinating actions during technical bridges. For the process to be effective, all updates and information regarding the incident must be fed to the MIM to update timelines and report
- Head of Service Ops – Is solely responsible for communicating, verbal and written, with RMG BU senior managers and POL management.

Communication Process Flow

- On suspicion or confirmation of MI, MIM to escalate to Service Ops SDM and Head of Service ops
- MIM to inform POL SD, via IMT, within 5 minutes of the service incident
- All updates to POL SD is via the IMT within agreed timescales controlled by the MIM
- MIM to issue SMS text to RMG BU alerting of potential issues – text to include date, time, nature of problems, severity, impact and name
- Head of Service Ops to inform the following within 10 minutes of the service incidents
  - RMG BU Ops Director
  - HNGX Program Manager
  - POL Senior Service Delivery Managers – Dave Hulbert and Gary Blackburn
- On confirmation from Head of Service Ops, MIM to send SMS text to POL Mgt D list if appropriate
- Head of Service Ops to coordinate and harmonise response to POL and RMG BU senior management
- Periodic (interval to be determined depending on issues but not more than 30 minutes for Major Incidents) SMS updates to be sent to the original SMS D list
- On final service restoration, an SMS text message must be sent to the original SMS D list
- Head of Service Ops to confirm understanding of incident closure with POL mgt and RMGA BU senior management and agree next steps
- MIM to continue liaising with IMT

Special Situations

Personnel Absence

- In the absence of Head of Service Ops, Ops SDM to deputise
- In the absence of both, a nominated individual would have been chosen before hand
- In the absence of the Program contact, a named person on the program to be informed

OOH

- The OOH duty manager will act as the MIM
- The Senior OOH duty manager will perform the role of Head of Service Ops

Duty Manager Change Over

FUJ00080189

- The Duty manager who started 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
- The Head of Service Ops to be informed, via text if OOH, of who the active MIM is