FUJ00080388

Document Title:	POA Operations Incident Management Procedure
Document Type:	Procedure Definition
Release:	Not applicable
Abstract:	This document describes the POA Operations Incident Management Procedure
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager
Author & Dept:	Tony Wicks – POA Operations
Internal Distribution:	Peter Thompson, Steve Bansal, Steve Gardiner, Steve Parker, Steve Evans, Changdev Pawashe, Andy Hemingway, Yannis Symvoulidis, Steve Godfrey, Jason Muir, Sandie Bothick, Bill Membery, Chris Harrison, Jerry Acton
External Distribution:	Debra O'Connell (Atos), Post Office Disaster Recovery Analyst Dave King, POL Security Manager
Security Risk Assessment Confirmed:	Yes

Approval Authorities:

Name	Role	See Dimensions for record
Steve Bansal	POA Senior Service Delivery Manager	
Sandie Bothick	POA MAC Team Manager	

Note: See Post Office Account HNG-X Reviewers/Approvers Role Matrix (PGM/DCM/ION/0001) for guidance.

FUJ00080388

0 Document Control

0.1 Table of Contents

FUJ00080388

FUJ00080388

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	16/10/06	First draft taken from CS/PRO/074. Updated to include HNG-X document references. Security Management appendix added Incident Management Process modified to reflect current working practises. Hardware and Network Call priorities referenced Problem Management escalation changed to SDM rather than Problem Initiator.	
1.0	06/11/06	Updated with comments following review of v0.1. Issued for approval	
1.1	02/03/07	Security Annex has been updated.	
2.0		Updated with comments following review of v1.1 Issued for approval	
2.1	14/04/09	Document updated names & job descriptions. Acceptance section added.	
2.2	16/04/2009	Version 2.1 is corrupt	
2.3	10/06/2009	Updated to incorporate PCI DSS and comments received from Connie G Penn.	
3.0	28/07/09	Issued for approval	
3.1	03/08/09	Updated to incorporate further comments received from Paul Halliden	
4.0	03/08/09	Issued for approval	
4.1	13/06/11	Updated to include clarified incident priority definitions and changed personnel names.	
4.2	30/06/11	Updated with comments following review of v4.1	
5.0	06-Jul-2011	Approval version	
5.1	23-Jan-2012	Update to include POLSAP and Security updates	
5.2	24-Oct-2013	Major update to align with Business Assurance Management procedures and for organisational changes.	
6.0	13-Nov-13	Incorporated changes for Sarah Hill HSD and issued for approval.	
6.1	11-Jun-14	Amended to replace the HSD function with the Atos Service Desk and replaced IMT references with the MAC team.	

FUJ00080388

		Also updated to reflect the introduction of Atos as POL's Service Integrator.	
6.2	26-Jun-14	Section 9.1 enhanced to include , and any Payment Brand incident (PCI)	
7.0	17-Jul-14	Incorporates minor amendments	
7.1	20 Oct-15	A major re-write to realign to the BMS Managed Incident procedure.	
7.2	23-Jun-16	Further major updates following a round-table review within POA on 3rd November 2015. Major amendments to Appendix A handling of security incidents.	
8.0	12-Jul-16	Incorporated minor changes for comments from the POA Senior Service Delivery Manager and issued for approval.	
8.1	20-Jul-2017	The procedure was checked for changes for CCNs 1602, 1609 and 16.14, no amendments were required. The distribution list was amended for organisational changes. Updated section 0.5.	
8.2	12-Sep-2017	Revised Appendix B, Contacts.	
9.0	12-Sep-2017	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Tony Wicks
Mandatory Review	
Role	Name
POA Senior Service Delivery Manager	Steve Bansal
POA MAC Team Manager	Sandie Bothick
POA Acceptance Manager	Steve Evans
POA Chief Security Officer	Steve Godfrey
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andy Hemingway
POA Business Continuity Manager	Almizan Khan
POA National Branch Issue & Comms Investigation Manager	Nick Crow
POA SDM Networks	Chris Harrison
POA SMC Manager	Jerry Acton
POA Security Manager	Jason Muir
POA Quality Compliance and Risk Manager	Bill Membery
POA Lead SDM Online Services	Yannis Symvoulidis

FUJ00080388

POA Problem Manager	Steve Gardiner
POA End User Services SDM	Chris Harrison
Post Office Ltd	
Security Manager	Dave King
ATOS	
Disaster Recovery Analyst	Debbie O'Connell

(*) = 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
SEC-3166	SEC-3285	9.5.2	Incident Categories

0.5 Associated Documents (Internal & External)

Reference	Version	Date	Title	Source
PGM/DCM/TEM/0001 (DO NOT REMOVE)			Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
CS/IFS/008			POA/POL Interface Agreement for the Problem Management Interface	Dimensions
SVM/SDM/PRO/0025			POA Problem Management Procedure	Dimensions
CS/PRO/110			POA Problem Management Database Procedures	Dimensions (PWY)
PA/PRO/001			Change Control Process	Dimensions
CS/QMS/001			Customer Service Policy Manual	Dimensions
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions
CS/REQ/025			Horizon HSD / SMC: Requirements Definition	Dimensions (PWY)
SVM/SDM/PRO/0001			POA Customer Service Major Incident Process	Dimensions
SVM/SDM/PLA/1048			SMC Business Continuity Plan	Dimensions
SVM/SDM/PLA/0031			Security Business Continuity Plan	Dimensions
SVM/SDM/PRO/0875			End to End Application Support Strategy	Dimensions
EMEIA Incident Management Process			EMEIA Incident Management Process	EBMS
#				EBMS
EMEIA Major Incident			EMEIA Major Incident Procedure	EBMS

FUJ00080388

Procedure				
EMEIA Root Cause Analysis (RCA) Process			EMEIA Root Cause Analysis (RCA) Process	EBMS
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
CISO	Chief Information Security Officer
CPP	Common Point of Purchase
FI	Forensic Investigator
HDI	Help Desk Interface (between Atos SDM12 and TfS incident management systems)
ICR	Initial Case Report
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KA	Knowledge Article also known as KEL
KEDB	Known Error Database
KEL	Known Error Log (in the context of this document, this is a workaround and diagnostic database) (Theses are also known as Knowledge Articles.)
MAC	Major Account Controllers (MAC team)
MSU	Management Support Unit
OLA	Operational Level Agreement
OMDB	Operational Management Database
ORF	Operational Review Forum
OTI	Open Teleservice Interface
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
PO	Post Office
POL	Post Office Limited
PSE	Product Support Engineers
RFC	Request For Change
POA	Post Office Account

FUJ00080388

SAN	Storage Area Network
SAP	Systems, Applications and Products (in Data Processing)
SDM(s)	Service Delivery Manager(s)
SDU	Service Delivery Unit
SISD	Service Integrator Service Desk (Atos Service Desk)
SLT	Service Level Targets
SMC	Systems Management Centre
SMT	Service Management Team
SRF	Service Review Forum
SRRC	Service Resilience & Recovery Catalogue
SSC	Software Support Centre
TfS	Triole for Service
UNIRAS	Unified Incident Reporting & Alerting System
VIP	VIP Post Office, High Profile Outlet

0.7 Glossary

Term	Definition
Common Point of Purchase	A location identified by card schemes as a single point where a number of stolen cards were used before the card was involved in fraudulent activity.
KELs and KAs	Note that different support teams refer to knowledge database information as either Knowledge Articles or Known Error Log. Where within this document KELs are referred to the reader can also consider them as Knowledge Articles.
Peak	The Incident Management System used by POA 3rd and 4th line support teams and other capability units involved in HNGX releases. It is linked with the TfS call management system.

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 Copyright

FUJ00080388

1 Introduction

1.1 Owner

The owner of the Incident Management process at the local POA account level is the Fujitsu POA Service Delivery Manager responsible for Incident Management within the POA account.

1.2 Objective

The objective of this document is to define the procedure for Incident Management in the POA environment. The procedure is the local implementation of the Fujitsu corporate Incident Management process (C-MSv1.3). Reference to process in this document is within the context of the corporate document C-MSv1.3. For the purpose of this document an Incident is defined as:

"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."

The quality of the service includes the protection of the confidentiality of business, personal and card data as defined by the POA Information Security Policy (SVM/SEC/POL/0003).

The document applies to all Incidents raised by the POA MAC or by SMC (out of hours or from systems monitoring tools), where they are related to the Fujitsu outsourcing contract. N.B calls presented to POA MAC / SMC that should be placed with the Atos Service Desk are transferred/ referred from POA MAC / SMC to Atos Service Desk.

For clarity; Post Office Limited (the customer) appointed Atos as their Service Integrator including the primary service desk function (Atos Service Desk, which may also be referred to as SISD).

The scope of the process is from the receipt of an incident by the MAC / SMC, through to the successful workaround or resolution of the incident.

For clarity, it should be noted that the MAC team are responsible for managing/owning Incidents between 08.00 and 20.00 Monday to Friday, 08.00 to 17.00 Saturday and Bank Holidays 0800 – 1400 excluding Christmas Day. The SMC assume this responsibility out of hours, i.e., outside these hours. The SMC are responsible for escalation of incidents to the POA OOH Duty Manager.

The key objectives of the process are (C-MSv1.3)

- Log, track and close all types of incident requests
- Respond to all types of incident requests
- Restore agreed service to the business as soon as possible
- Resolve incidents within the target timescales set for each priority level within the Service Level Agreement(s)
- Resolve a high number of requests at first contact
- Ensuring incident priorities are linked to business priorities
- Keeping the user informed of progress
- Reduced unplanned downtime
- Improved Customer satisfaction

1.3 Process Rationale

The primary goal of the Incident Management process is to restore normal service operation as quickly as possible, thereby minimising adverse impact to the business. In turn, this ensures the highest level of service quality and availability. Normal service operation is defined here as service operation within Service Level Targets (SLT).

FUJ00080388

Demonstrating a professional approach to Atos, the Service Integrator contracted to POL, and Post Office Limited (the customer) and their clients.

1.4 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 and 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 SMC acts as the first point of contact.
- Any activity detailed in this document which is assigned to the MAC is handed over to the SMC outside the MAC Core Hours.

FUJ00080388

2 Inputs

The inputs to this process are:

- All Incidents reported by Contact with the MAC / SMC. Contact is defined as voice, e-mail, incident transfers over the HDI interface from the Atos Service Desk or Tivoli Alert as the methods of communication with the MAC / SMC and fall into the following categories:
  - Business process error
  - Hardware or software error
  - Request for information e.g. progress of a previously reported Incident
  - User complaint
  - Network Error
  - Logging via HNG-X web interface
- Severity and SLT information.
- Evidence of an Error.
- System Alerts received automatically from transaction monitoring tools. Due to the urgent nature of some of these alerts, they may be dealt with directly by SSC, with an update of workaround or resolution supplied to MAC / SMC. It should be noted that these alerts enter the process at step 1.2.3, and are not subject to prior steps in 1.1 & 1.2 of this process.

FUJ00080388

3 Risks and Dependencies

3.1 Risks

The following define the risks to the successful delivery of the process:

- Break in the communications chain to third parties. Mitigation is to invoke escalation procedures.
- Non-availability of the MAC / SMC Incident Management System. Mitigation is given in the MAC / SMC Business Continuity Plan.
- Non-availability of the HDI interface with the Atos Service Desk.
- Non-availability of the OTI links to internal & external service desk tools.
- Lack of information given to the MAC / SMC regarding changes, Atos or POL Business updates, request for changes, status of Problems etc. Processes must be followed to lessen this risk, such as the Change Management and Problem Management Processes.
- Unavailability of sufficient support unit staff
- Unavailability of sufficient tools for Incident diagnosis
- Non-availability of KEL or call management systems
- The provision of inadequate staff training within the MAC / SMC, SDU's or 3rd party suppliers
- Unavailability of systems for evidence gathering.

3.2 Dependencies

This process is dependent on:

- Effective Incident handling by the MAC / SMC
- The known error information being available and kept up to date with all errors as the root cause becomes known to Problem Management
- Knowledge database kept up to date with POL business and services knowledge
- Fujitsu infrastructure support of the MAC / SMC tools
- Appropriate training plans / skills transfer of desk agents.
- Appropriate training needs to include hardware, software and networks support staff, SDU's and 3rd party suppliers
- Effective routing of calls to SDUs and third parties
- Effective escalation procedures and the maintenance thereof within Fujitsu, POL and third parties
- Governance of Incident / Problem Management procedures
- Effective feedback to POL through Service Management SRFs, contributing to end user education and reduced Incident rates.
- Internal feedback to improve the Incident / Management Process.
- SLT and OLA knowledge and understanding across all Fujitsu and 3rd party support
- POA, SDU and 3rd party consistent co-operation in incident identification and resolution

FUJ00080388

4 Resources

The resources required for this process are:

- Process Owners
- Major Account Controllers team
- Service Management Team
- System Management Centre team
- SSC
- SDUs
- Triole for Service incident management system
- Peak
- SDM12 (within Atos) and the HDI interface into TfS.
- OTI links
- TIVOLI
- Additional remote Management, Operational and Diagnostic tools
- Detailed Process and Procedure documentation

4.1 Roles

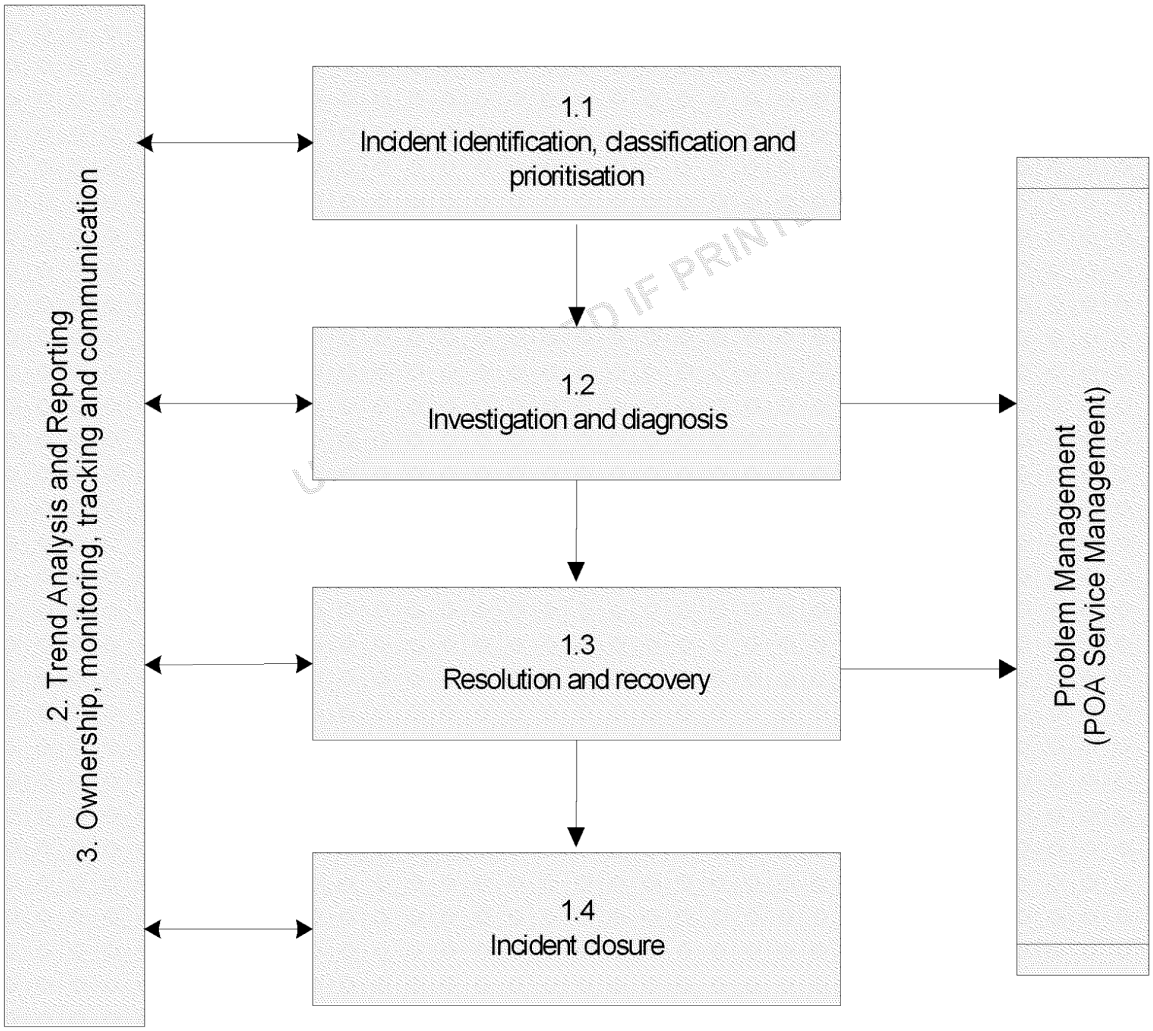
The main roles required by the process are:

- Incident Manager - To drive the Incident Management process, monitor its effectiveness and make recommendations for improvement. The key objective is to ensure that service is improved through the efficient resolution of Incidents.
- Service Desk Agent - To provide a single point of contact for users, dealing with the management of routine and non- routine Incidents, Problems and requests
- Incident Resolver - To accurately diagnose and resolve Incidents and Problems within SLA, and to assess, plan, build/test and implement Changes in accordance with the Change Management Process. This role will typically be fulfilled by the support teams and service delivery units.

FUJ00080388

5 Process Flow

5.1 Level 1 Incident Management Process



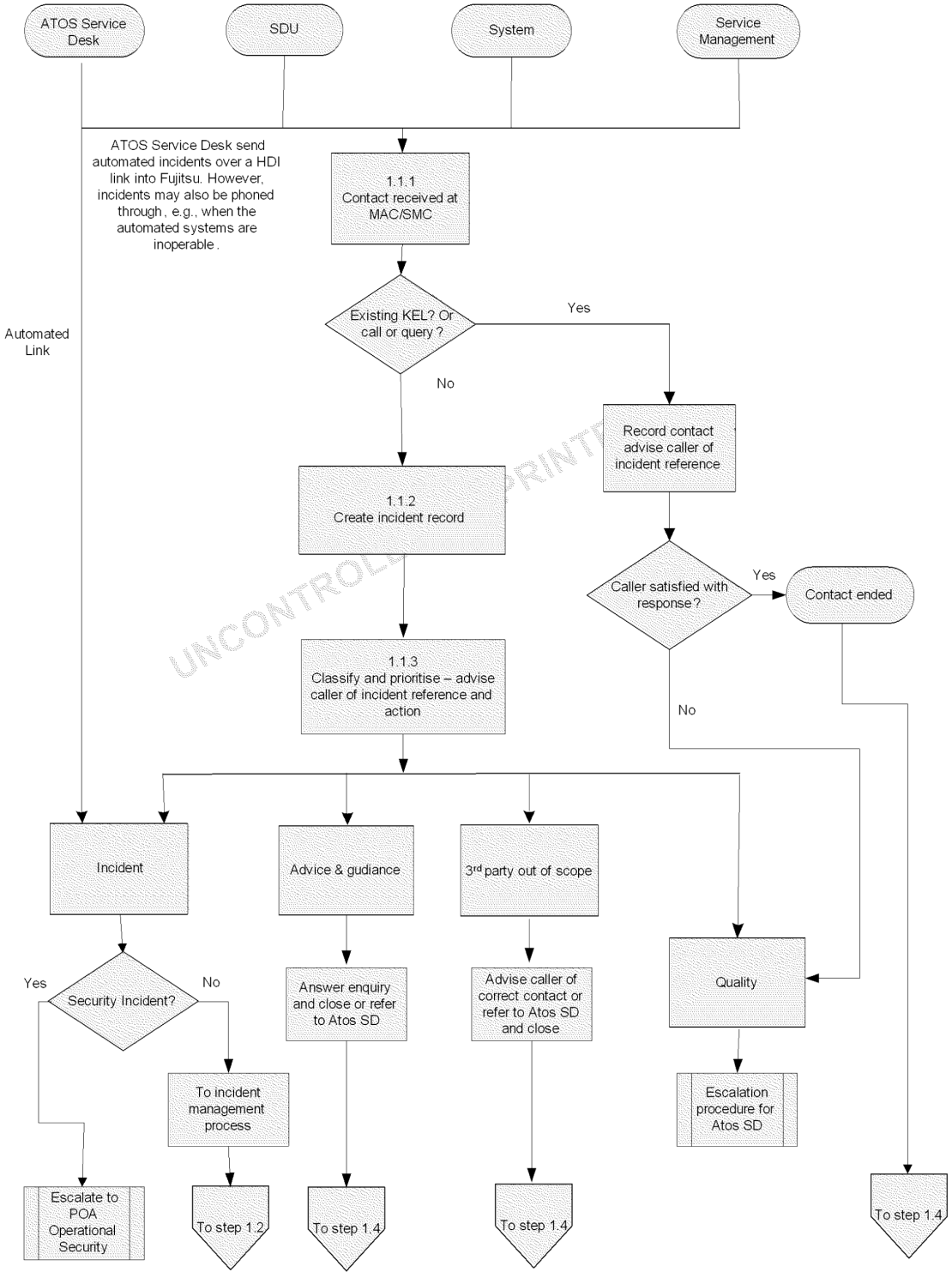
FUJ00080388

5.2 Level 2 Incident Management Processes

5.2.1 Step 1.1: Incident identification, classification and prioritisation

Responsible: MAC / SMC, users, SDU's, Service Management

FUJ00080388



FUJ00080388

1.1	Incident Identification, Classification and Prioritisation			
Step No	**Current Situation/Input**	**Activities**	**Accountability Responsibility**	**Next Step**
1.1.1	Incident Identification and Logging	An Incident is received through contact (see definition in Section 2.0 above) with the MAC / SMC from: Atos SD Fujitsu SDUs POA IT Service Management Third Parties Fujitsu Service Delivery Management Post Office Ltd, including POL Information Security For Ownership, Monitoring, Tracking and Communication by the MAC/SMC/SSC see section 5.2.6 below The caller may be enquiring about an existing Known Error or Incident. Check the Knowledge Database for an existing KEL which provides avoidance actions. For existing incidents the details are provided and if the response is satisfactory, contact is ended, moving the incident to step 1.4. If the caller is not satisfied with the response, the relevant Escalation Procedure is invoked. In cases of Incidents that are either taking an above average time (for this type of Incident) to resolve or involve multiple SDU's, the MAC / SMC alerts the relevant Service Delivery Manager to provide focused management of the Incident. Outputs: Service desk complaints procedure invoked, an existing incident updated or new incident validated	See specifics under Activities	1.1.2
1.1.2	Create Incident Record	For a new Incident, Contact details are recorded if not system generated, e.g., an Atos SD SDM12 incident. Details taken are dependent upon the error reported. Typically they may include: The user's name and unique ID number Location and contact details Alternative contact details (where appropriate) Hardware details as appropriate Software error details, including application use at point of failure where known Business and User Impact Description of Incident Location access times Supporting evidence, e.g., log files, screen shots, etc. Output: Incident record created	MAC, SMC	1.1.3
1.1.3	Classify and Prioritise the incident	Classification of Call determined as one of the following: Error Incident – invoke Incident Management Process Step 1.2 Quality – record details of complaint or compliment and	MAC, SMC	1.2 or 1.4

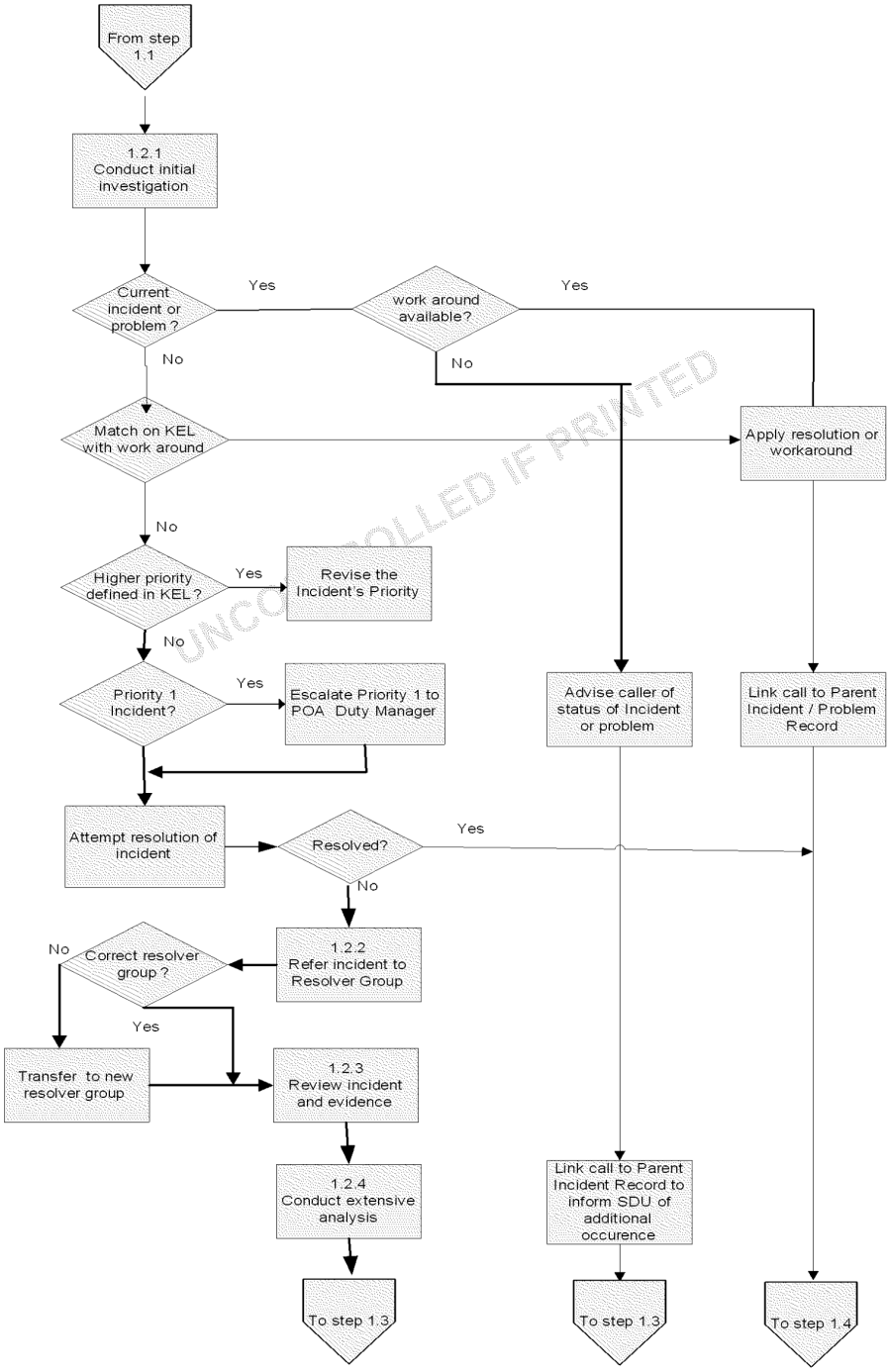
FUJ00080388

		invoke the relevant Escalation Procedure. Advice & Guidance – Cold Transfer to Atos SD. Out of scope – if the call is not within scope for the services provided by Fujitsu advise the caller of the correct number or refer to Atos SD and close incident. Set Priority of the incident either based on the priority documented in an existing KEL or based upon the Urgency and Impact of the incident, refer to POA Incident Enquiry Matrix. (Re-assess the caller's assessment of the impact of the incident, e.g., number of users affected and business impact, and contact the POA Duty Manager if clarity is required regarding the priority.) Consider if the incident is out of scope, e.g., the incident description indicates that a third party is responsible. Consider if the incident being reported is a Security Incident and classify and manage under the POA Operational Security process (See Appendix A for guidance). Consider if the incident is for chargeable work, e.g., file re-sends. When applicable continue raising the incident and advise the POA Duty Manager. Ensure all third party references are detailed in the TfS incident and it is clearly documented when the incident is transferred to a third party for investigation. If the incident is considered a Major Incident as defined in SVM/SDM/PRO/0001 Major Incident Process, the Major Incident Procedure is invoked inform the POA Duty Manager. Provide the caller with the incident reference. Output: Prioritised and updated incident record		

FUJ00080388

5.2.2 Step 1.2: Investigation and Diagnosis.

Responsible: MAC / SMC



FUJ00080388

1.2	Investigation and Diagnosis.			
Step No	**Current Situation /Input**	**Activities**	**Accountability/ Responsibility**	**Next Step**
1.2.1	Incident record	Conduct Initial Investigation. The MAC / SMC agent should check the TfS Incident and problem database for current outstanding incidents or problems. If a match is made, the caller is then advised of the status of the incident or problem and the master record (parent incident or problem record) is updated to reflect the current occurrence. The MAC / SMC agent should then attempt to resolve the Incident using the resources available. This starts by the MAC / SMC interrogating the KEL knowledge database and support documentation to find all information related to the Incident symptoms. If the Incident is routine, i.e. there is a predetermined route for resolution, then the Incident is resolved on the call or referred to the relevant SDU using the MAC / SMC Support Matrix. Note: If a KEL recommends setting a priority of an incident at a priority higher than that specified in the POA Incident Enquiry Matrix then revise the incident to the higher priority. Output: Updated incident with initial investigation findings or input incident resolution detail (go to step 1.4)	MAC, SMC	1.2.2 or 1.4
1.2.2	Refer to Support Matrix and transfer to appropriate SDU	Refer the incident to Resolver Group Where there is no resolution to the Incident the MAC /SMC agent should transfer the incident to the relevant Service Delivery Unit (also known as Resolver Group) using the MAC / SMC Support Matrix. MAC are appraised of the position. Note: When incidents are transferred to the Software Support Centre (EDSC) the TfS incident is transferred into a Peak incident system. Within Peak the incident priorities are defined as A, B, C and D. Therefore, when transferring TfS incidents into Peak ensure the following is adhered to: TfS priority 1 equates to Peak priority A TfS priority 2 equates to Peak priority B TfS priority 3 equates to Peak priority C TfS priorities 4 and 5 equates to Peak priority D If it this cannot be achieved through automation the MAC or SMC Agent undertaking the transfer is to log a comment on the TfS incident stating the TfS and Peak priorities. Output: Updated incident transferred to relevant Resolver Group	MAC, SMC	1.2.3
1.2.3	Incident and evidence	Review Incident. The referred SDU investigates and diagnoses the Incident,		1.2.4

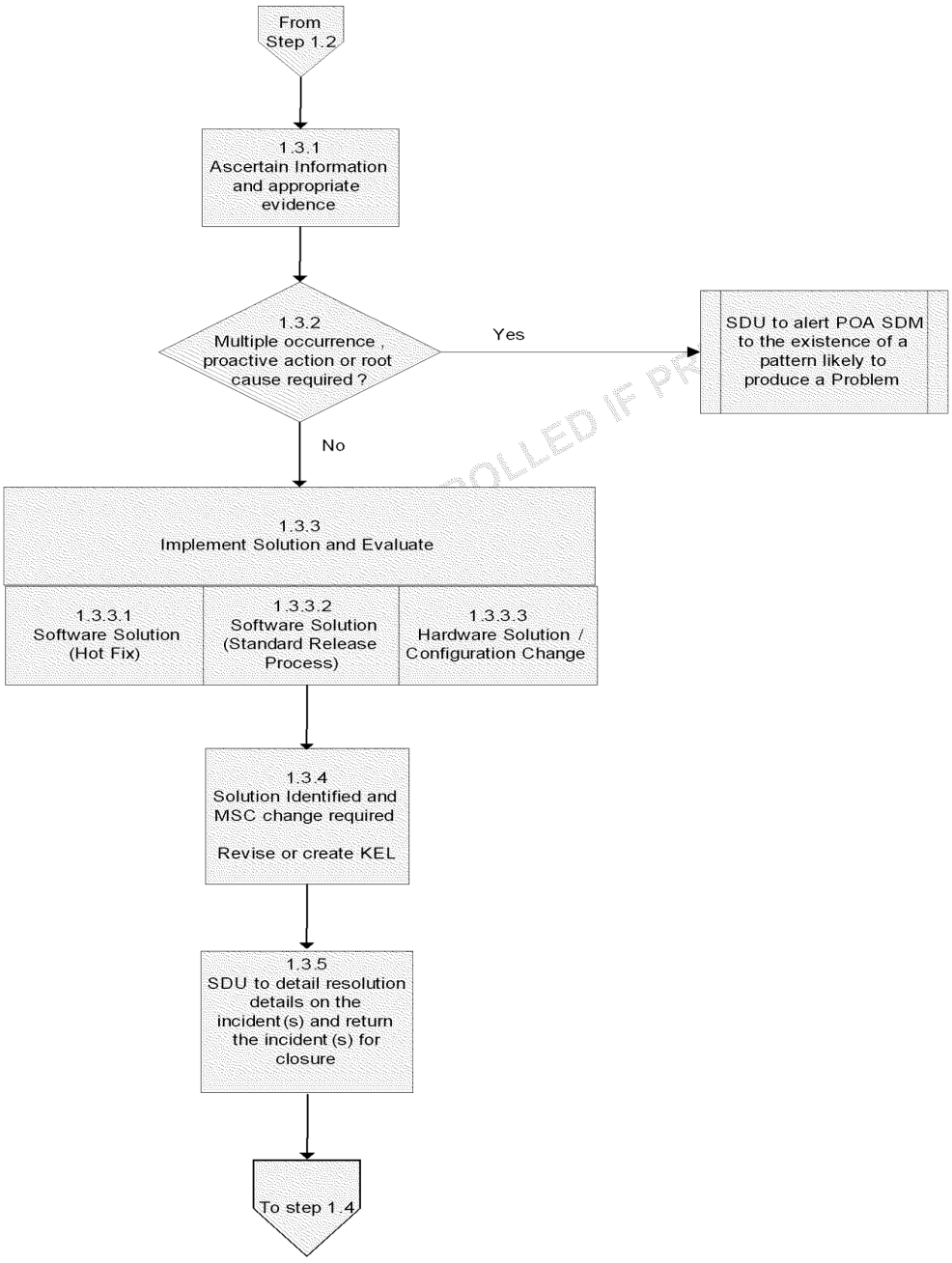
FUJ00080388

		based on information already taken by the MAC / SMC. Consider if the incident should have been assigned to an alternative SDU. If it is more appropriate for an alternative SDU to investigate, 'voice' the team and then re-assign the incident. Consider if the appropriate Impact, Urgency and Priority has been set for the incident (e.g., based on the fault and the SLTs for the affected service(s). Revise when necessary. The SDU should review the analysis and re-consider if there are any related incidents, problem or KEL knowledge entries. Consideration should be given to any recent changes, e.g., Manage System Changes or Software Releases which could either cause or contributed to the new incident. Output: Updated incident (KELs/Changes, etc. considered) and possible transfer to alternative Resolver Group		
1.2.4		Conduct Extensive Analysis. If the incident is deemed the same as an existing master incident add it as a child incident and return incident to MAC / SMC team. (return to step 1.2.1) The referred SDU investigates and diagnoses the incident, based on information already taken by the MAC / SMC, together with any new information. The SDU also coordinates where sub-contract third parties are involved. If the Incident has no associated KEL, or it is complex and involves multiple SDU's, or if it has been unresolved for an extended period, the MAC will alert the POA Service Delivery Manager to the existence of a pattern likely to produce a Problem. Consider if there is sufficient evidence and it is of the correct type for the incident to be investigated. If not detail the required evidence so the incident can be returned to the initiator. Consider if the incident needs to be referred to a third party vendor/supplier. If applicable ensure the Service Delivery Manager responsible for the relationship with the third party supplier is aware of the incident. From the output of the analysis the SDU diagnoses the cause and identifies a solution or workaround. Output: Incident updated, further evidence requested, transfer to third party or solution/workaround identified.	Second line support stage. SDU investigation	1.2.1, 1.3.1 or 1.4

FUJ00080388

5.2.3 Step 1.3: Resolution and Recovery

Responsible: SDU's



FUJ00080388

1.3	Resolution and Recovery			
Step No	**Current Situation/ Input**	**Activities**	**Accountability/ Responsibility**	**Next Step**
1.3.1	Further incident information required.	Ascertain Information. If further evidence, information is required request this from the incident initiator and update the incident with the requested evidence details and suspend the incident detailing the date and time when it is to be unsuspended. If the incident initiator is unavailable or uncontactable update the incident with these details and suspend the incident detailing the date and time when it is to be unsuspended. When the un-suspension time is reached contact the incident initiator to obtain the additional information and unsuspend the record. Output: Update incident detailing required evidence	SDU / MAC/SMC	1.2.1
1.3.2	Multiple new incidents.	Raise Problem Record Where it is identified that there are multiple incidents for the same unexpected event with no known resolution a problem record should be raised. See section 2.1 of SVM/SDM/PRO/0025 for further details. Note: As ATOS Service Desk are the primary service desk for Branch incidents they should be highlighting where there are multiple incidents for the same unexpected event. Outputs: Updated incident and the issue being investigated through the Problem Management procedure.	SDU / MAC/SMC	1.3.4
1.3.3	Solution identified	Implement Solution and Evaluate.		
1.3.3.1	Solution identified	Software Solution Required – Hot Fixes Where it is identified that a code fix is required and it is a high priority incident for which the POA Senior Management or POA Problem & Major Incident Team recommend a 'Hot Fix' is required POA Account shall hold an emergency Business Impact/Peak Targeting Forum meeting to agree that the change should be released as a Hot Fix. (Note: the production, testing and release of 'Hot Fixes' should be in exceptional circumstances as the activity impacts the normal planned activities.) Outputs: Updated incident and Hot Fix being released through documented processes.	SDU/POA P&MI	1.3.4
1.3.3.2	Solution identified	Software Solution Required – Standard Release Process Where it is identified that a code fix is required via the standard Release process the incident (Peak) is to be updated with Impact details, and details of any fault circumvention. POA Release Management schedule the incident to be reviewed at a Business Impact Forum to review and agree if a	SDU/POA P&MI	1.3.4

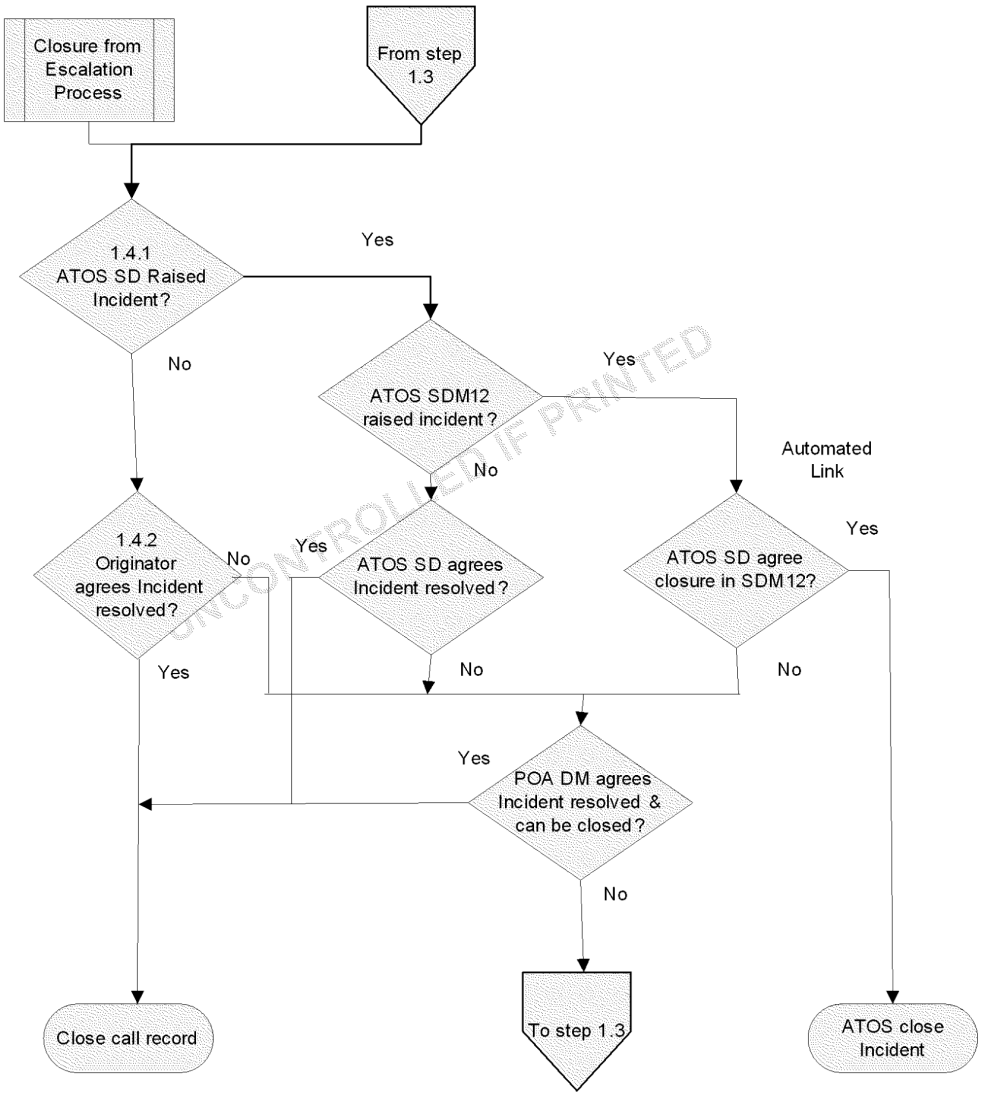
FUJ00080388

		software fix is to be developed or the circumvention implemented. If the BIF forum agrees that a formal fix is required the Incident (Peak) is scheduled into a subsequent Peak Target Forum so that an appropriate release is identified for the change. Individual releases are managed through a controlled Integration, Live System Testing and release to live processes via the Managed Service Change process. If the Business Impact Forum decides the incident does not require a formal fix and a circumvention is available, a Knowledge Entry Log can be raised and the incident can be resolved using the work around details. Outputs: Updated incident and a fix being released through documented processes.		
1.3.3.3	Solution identified	Hardware Solution or Configuration Change Required. Where an incident can be resolved via a hardware component replacement, e.g., faulty router, or a configuration change, e.g., revising IP address in firewalls (which cannot be tested in a test environment) then the incident should be updated with the solution details and cross reference made to the Managed System Change identifier under which the change is going to be made. Outputs: Updated incident and correction being implemented through documented processes.	SDU/POA P&MI	1.3.4
1.3.4	Solution identified and change required	Raise a Change Record (Linked with 1.3.3) Where it is identified that a change to the infrastructure or to a configuration item is required, including 'Hot Fixes' then a Managed System Change should be raised. Ensure the incident contains the MSC reference (and the MSC details the TfS incident reference). SDU/SMC ensure either the applicable KEL(s) is/are updated with the solution details or that a new KEL is raised. See SVM/SDM/PRO/0875 section 11.0 for Knowledge Database information and the creation and maintenance of KELs. Suspend the incident, detailing the date and time, until the MSC change has been implemented.	SDU/POA P&MI	1.3.5
1.3.5	Resolve Incident	The SDU should detail on the incident the resolution details including details of any hot fix or release the fix has been made in and details of any Managed Service Change. The SDU should also include the references of Knowledge Entry Logs that have been created or updated relating to the incident(s). The MAC/SMC should ensure that Parent Incident contains all applicable information so that there is an audit trail from all child incidents.	SDU/POA P&MI	1.4

FUJ00080388

5.2.4 Step 1.4: Incident Closure

Responsible: MAC / SMC



FUJ00080388

1.4	INCIDENT CLOSURE			
Step No	**Current Situation/ Input**	**Activities**	**Accountability / Responsibility**	**Next Step**
1.4.1	MAC managed incidents	For incident raised by the MAC for the Atos SD the MAC will liaise with the Atos SD and POA Duty Manager on the closure of the incident. If closure is not agreed the incident shall be returned to the SDU to be reworked. For those incidents raised in an external domain by the Atos SD on SDM12 and transferred to TfS over the HDI link the Atos Service Desk are responsible for closing these. In the event of any exceptions to this the MAC and SMC teams are to raise the incident details to the POA Duty Manager. For incident raised by the SMC/MAC for external suppliers to Fujitsu the SMC/MAC shall close the incidents when they are content the issue has been resolved. In the event of any exceptions to this the MAC and SMC teams are to raise the incident details to the POA Duty Manager. If closure is not agreed the incident shall be returned to the SDU to be reworked. Output: Updated incident returned to SDU or incident closed after agreement received.	MAC	1.2.3 or 1.4.2
1.4.2	MAC/SMC managed incidents	The incident may now be closed with the agreement of the originator. If closure is not agreed the incident shall be returned to the SDU to be reworked. When a Parent incident has been raised as a result of multiple user incidents, e.g., Post Masters, Horice users, etc, ensure an adequate number of child incidents are closed with the requestors' agreement before closing the Parent incident. (Guideline: 10 agree closure of 10 sample child incidents.) Where incidents are linked to a Major Incident ensure they are updated with the resolution details or have a cross reference to the Major Incident Report document reference which is to be stored in Dimension. Outputs: Incident or major incident closed after agreement received or parent incident closed after agreement on a sample of child incidents	MAC, SMC	End

FUJ00080388

5.2.5 Step 2: Trend Analysis and Reporting.

2	Trend Analysis and Reporting			
Step No	**Current Situation/ Input**	**Activities**	**Accountability / Responsibility**	**Next Step**
2.1	MAC SMC	Trend Analysis On a monthly basis the SMC (and on behalf of the MAC team) shall undertake a trend analysis of the incidents raised, the prioritisation of the incidents and feedback on the resolution. This input is to be submitted to monthly service reviews. The analysis should cover: Incident volumes over a six month period showing monthly open and closed incidents, Incident stack management and incident management within Resolver Groups over the month Overview details of the individual Priority 1 incidents. Outputs: Monthly trends analysis that are fed into the monthly reports.	MAC	2.2
2.2	MAC SMC	Reporting On a monthly basis the SMC shall submit a SMC Service Review pack containing the above incident analysis for a review by the Service Delivery Manager and Problem and Major Incident Manager and for review by senior account managers and the customer if required. The POA Operational Services team shall produce a monthly Service Management Review Report which shall list service impacting incidents derived from the P&MI Team Virtual White Board. The report is to include feedback on incidents resulting from the introduction of new services and provide an overview of the service impacting incidents. Outputs: SMC Service Review Report and Operational Services Service Management Review Reports.	MAC, SMC	End

FUJ00080388

5.1.6 Step 3: Ownership, Monitoring, Tracking and Communication

Responsible: MAC / SMC, SSC

3	Ownership, Monitoring, Tracking and Communication			
Step No	**Current Situation/ Input**	**Activities**	**Accountability / Responsibility**	**Next Step**
3.1	MAC SMC	Ownership, Monitoring, Tracking and Communication Throughout the Incident, the MAC / SMC retains ownership for monitoring and keeping the call raiser informed of progress, unless the incident is specifically software related, in which case SSC hold the responsibility for confirming details of closure The MAC / SMC manages the complete end-to-end Incident process. Activities include: Regularly monitoring the status and progress towards resolution of all open Incidents Give priority for Incident monitoring to high-impact Incidents Keep affected users informed of progress without waiting for them to call, thus creating a pro-active profile Monitors SLT and escalates accordingly. If an Incident has no associated KEL or, it is complex and involves multiple SDU's, or if it has been unresolved for an extended period, MAC will alert the POA SDM to the existence of a pattern likely to produce a Problem. Updating MAC / SMC TfS Knowledge Articles from information supplied from SSC KEL. This may be applied as a direct copy or amended for use by the agents, dependent upon the technical complexity of the update.	MAC	End
1.3.2	MAC SMC	Alerting Post Office Account have an account specific process for alerting. The MAC team achieve incident monitoring and alerting by constant monitoring of the incident stacks and conduct checks during core hours on a 15 minute basis. ATOS have enable the alerting feature within SDM12 for incidents raised in their domain and monitor alerts for those incidents. Outputs: The MAC team advise the Service Desk SDM when there is a risk of incidents exceeding agreed SLTs.	MAC, SMC	End

FUJ00080388

6 Outputs

The outputs from this process are:

- A Problem referred to the Service Delivery Manager with line of business responsibility, where there have been one or more Incidents for which the underlying cause is unknown
- An update to the Knowledge Database
- A workaround or permanent resolution for a hardware, software or network error
- An answer to a question from a user
- The receipt and onward transfer of information received by the MAC / SMC
- A service improvement recommendation.
- Change of operations procedures.
- Change of Business Continuity Plan (BCP) priorities and documentation.

Where appropriate:

- Monthly Report on all PCI minor incidents
- ICR (Initial Case Report)
- Record in the Incident Security Log

FUJ00080388

7 Standards

This Process conforms to:

- Process Management and Control PA/PRO/038
- ITIL Best Practice
- BS15000
- BS9001
- BS/ISO IEC 27001
- IEC 17799:2005
- PCI DSS version 1.2

FUJ00080388

8 Control Mechanisms

The contractual measures that apply to this service are described in the Service Desk Service Description (SVM/SDM/SD/0001)

This covers service availability, service principles, service definition, incident prioritisation, service targets and limits and MAC / SMC performance reporting.

In addition, internal measures may apply for specific productivity and service improvement activities.

FUJ00080388

9 Appendix A: Security Incident Reporting

9.1 Scope

This annex contains **guidance** regarding the reporting and investigation of security incidents concerning the HORIZON Network, POA and any Payment Brand incident (PCI).

9.2 Aim

The aim of this guidance is to ensure that the reporting routes for Security Incidents are kept as simple as possible and that investigations are managed in an efficient and auditable manner.

9.3 Changes

This guidance is primarily for use by the MAC team, the POA Security Team, the POL Security Team, and SSC staff. The SecOps team also have their own work instructions for handling security incidents and there is also an overarching Information Security Incident Management Procedure ISSC-11a.

All incident documentation is subject to review and update by the business continuity and information security teams as part of the lessons learnt process following an incident and following the annual review of the incident process as part of business continuity.

9.4 POL Incident Handling Guidance

All POL incidents will still be handled in accordance with existing POL/ATOS guidelines. This document does not replace these or, indeed, replace any part of the content rather it details POA guidance on handling security incidents.

9.5 IT Incidents

9.5.1 Incident Definition

9.5.1.1 An information security Incident is: "an adverse event or series of events that compromises the confidentiality, integrity or availability of Fujitsu Services Post Office Account information or information technology assets, having an adverse impact on Fujitsu Services and/or Post Office Ltd reputation, brand, performance or ability to meet its regulatory or legal obligations." This will also extend to include assets entrusted to Fujitsu including data belonging to Post Office Ltd, its clients and its customers.

9.5.2 Incident Categories

Incidents can be categorised in many ways, they can occur alone or in combination with other incident categories and can vary significantly in severity and impact. It is important that all incidents are recognised and acted upon.

9.5.2.1 For the purpose of illustrating the impact of incidents two levels of severity have been defined (Note: in practice the assessment may be less straightforward):

FUJ00080388

A MINOR incident will normally have limited and localised impact and be confined to one domain, resulting in one or more of the following:

- Loss or unauthorised disclosure of internal or sensitive material leading to minor exposure, or minor damage of reputation
- Loss of integrity within the system application or data, leading minimal damage of reputation; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery
- Loss of service availability within the domain, leading to reduced ability to conduct business as usual; negligible loss of revenue; minimal loss of customer / supplier / stakeholder confidence; negligible cost of recovery
- Individual attempts to breach network security controls shall be treated as a minor security breach.
- Subject to discussions with the POA Duty manager due to high volume of calls relating to the same type of incident it may well be a requirement to follow the POA Major Incident Process (SVM/SDM/PRO/0001) following the advice from the POA Duty Manager.

A MAJOR incident will have a significant impact on the Network Banking Automation Community resulting in one of more of the following:

- Loss or unauthorised disclosure of confidential or strictly confidential material, leading to brand or reputation damage; legal action by employees, clients, customers, partners or other external parties
- Loss of integrity of the applications or data, leading to brand or reputation damage; loss of customer / supplier / client confidence; cost of recovery
- Loss of service availability for applications or communications networks, leading to an inability to conduct business as usual; loss of revenue; loss of customer / supplier / client confidence; cost of recovery
- A concerted attempt or a successful breach of network security controls shall be treated as a major security breach.

NB. For a Major Incident the POA Major Incident Process (SVM/SDM/PRO/0001) should be followed.

9.5.3 Examples of IT Incidents

- Theft of IT equipment / property, including software
- Malicious damage to IT equipment /property, including software
- Theft or loss of Protectively Marked, caveat or sensitive IT Data.
- Actual or suspected attacks on the Fujitsu Services POA Network or Information System.
- Potential compromise of systems or services at the Data Centre through evidence retrieved and presented by Police or POL's card acquirer.
- Attacks on Fujitsu Services Post Office Account personnel via Information Systems. (I.e. Harassment, Duress.
- Malicious/offensive/threatening/obscene emails.
- Obscene phone calls

FUJ00080388

- Breaches of software licensing
- Virus attack and other malicious code attacks
- Hacker attacks
- Terrorist attacks
- Insider attacks
- Competitive Intelligence gathering (Unethically)
- Unauthorised acts by employees
- Employee error
- Hardware or software malfunction
- Suspected Fraudulent Activity
- Specific compromise of card data.

The above list is a non-exhaustive list of examples. Any other IT related incidents reported, will be considered and passed to the appropriate authority for action.

9.5.4 Containment

Whenever an Incident is identified which presents a serious threat to conduct normal business it should be contained and isolated as quickly as possible. This will mean platforms that appear to have suffered virus attack or other malicious code attack need to be quarantined immediately to prevent further spread. It may also be necessary to isolate network connections that appear to be the source for Denial of Service threats or where they have been subjected to suspected hacking attack.

If the incident relates to card data, the environment may be subject to a Forensic Investigation imposed by POL's merchant acquirer. In this instance log data will need to be reviewed and analysed.

9.6 Reporting

Whenever a security incident is identified which presents a serious threat to conducting normal business it is contained and isolated as quickly as possible.

A security Incident is first notified to either the MAC or SMC Team, then transferred to the SecOPs call stack, once it is initially assessed as a Security Incident by MAC/SMC.

Security Incidents may also be reported directly into the POA SecOps team via the reporting button on the POA Portal. It is important to allow the 2 reporting methods, as some staff may want to report some types of security incidents directly to the SecOps team. In accordance with the Fujitsu Security Policy Manual Section 16, the reporting routes must be kept as simple as possible. The initial report will be validated and clarified by SecOps, with calls made to the initiator if more information is required. SecOps will follow team work instructions to progress their investigation.

All Security Incidents are to be reported to the SecOps team via a dedicated mailbox and escalated by phone if necessary. Depending on the type of Incident and the severity of the incident, POA Security makes the decision to escalate details to the POL/ATOS Security teams. In the case of Data Centre incidents, POA Security also informs the Data Centre.

Regardless of the severity of the incident, when a compromise in card data occurs, the incident is reported to POL Security so that POL can comply with its contractual obligations with its card acquirer.

FUJ00080388

The investigation of a reported incident is carried out by a nominated investigator from the POA SecOps team. ATOS and POL Security Teams will be on hand to provide support as required and in accordance with the POL/ATOS Information Security Incident Management Procedure. The investigator will obtain as much original evidence as possible to ensure that is admissible in court, if required.

Following the initial investigation and where considered appropriate, the appropriate senior manager within POL liaises with the local Police or other external agencies.

When an investigation is closed the POA Security Manager seeks to ensure that details of the investigation have been recorded and can be made available for Route Cause Analysis, trending & lessons learned.

9.7 Investigation

9.7.1 Policy

Although all security incidents will initially be reported to the POA Security Manager in order to have one point of contact for all parties, some or all of the investigation requirements may be passed to one or more of the following for further action. The decision of delegation will be determined by the POA Security Manager in association with POL Information Security Incident Manager.

9.7.2 POL Security / Investigation Team

9.7.2.1 In the event that the reporting of an incident is passed to ATOS Security or the Investigation Team, details of the investigation, and final outcome or reference details, should be added to the TfS call which be communicated to ATOS. It is important that for any incident investigated the correct procedures are adopted regarding evidence, as the information collected and recorded may be used for evidential purposes at a later date.

9.7.2.2 In the event that the POA Security Team takes ownership of an investigation, they will report the results to ATOS.

9.7.2.3 During any investigation the Investigator must comply with the appropriate legislation and compliance requirements and regulatory or standard requirements.

9.7.2.3.1 All initial investigations should be carried out at the earliest opportunity and any queries should be directed to POA Security Manager. Investigation must be reliable, stand up to scrutiny and potential cross-examination and evidence must be properly obtained, recorded and time stamped.

9.7.3 External Investigator

9.7.3.1 Should it be considered necessary the incident might be passed to an external Investigator or forensics team, who will ensure that any data required for evidential purposes is captured and investigated using a systematic approach which ensures that an auditable record of evidence is maintained and can be retrieved. In some cases, where a compromise to card data is involved, two Forensic Investigation teams may be involved. One team operating on behalf of POL gathering the required audit logs to use to analyse and investigate the problem. A second Forensic Investigations team

FUJ00080388

may be imposed to investigate on behalf of the card acquirer and card schemes. In all incidences where a Forensic Investigation is involved, the Forensic Investigators will be shadowed by POL's Legal and Security Teams.

9.7.4 Evidence Rules

9.7.4.1 Rules of Evidence

Before undertaking security incident investigation and computer forensics it is essential that investigators have a thorough understanding of the Rules of Evidence. The submission of evidence in any type of legal proceedings generally amounts to a significant challenge, but when computers are involved the problems are intensified. Special knowledge is needed to locate and collect evidence, and special care is required to preserve and transport evidence. Evidence in computer crime cases differs from traditional forms of evidence in as much as most computer related evidence is intangible and is in the form of electronic pulse or magnetic charge, hence the need to use specialist teams. That said the information collected and recorded from the Operational areas is equally important and must be recorded with due care and diligence.

9.7.4.2 Types of Evidence

Many types of evidence can be offered in court to prove the truth or falsity of a given fact.

The most common forms of evidence are Direct, Real, Documentary and Demonstrative.

Direct Evidence

Direct evidence is oral testimony whereby the knowledge is obtained from any of the witness's five senses and is in itself proof or disproof of a fact in issue. Direct evidence is called to prove a specific act such as an eye witness statement.

Real Evidence

Real evidence also known as associative or physical evidence is made up of tangible evidence that proves or disproves guilt. Physical evidence includes such things as tools used in the crime, and perishable evidence capable of reproduction etc. The purpose of physical evidence is to link the suspect to the scene of the crime. It is that evidence that has material existence and can be presented to the view of the court and jury for consideration.

Documentary Evidence

Documentary evidence is presented to the court in forms of business records, manuals, printouts etc. Much of the evidence submitted in a computer crime case is documentary evidence.

Demonstrative Evidence

Demonstrative evidence is evidence used to aid the jury. It may be in the form of a model, experiment, chart or an illustration offered as proof.

9.7.5 Process

In most cases response to a reported incident the initial investigation will be carried out by a nominated investigator normally the POA Security Manager or a member of the SecOps team. ATOS and POL Security Teams will be on hand to provide backup and assistance if required. When seizing evidence from a computer related crime the investigator will collect any and all physical evidence such as the personnel computer, peripherals, notepads and documentation etc., in addition to computer generated evidence.

There are four types of computer generated evidence:

FUJ00080388

- Visual output on a monitor.
- Printed evidence on a plotter.
- Printed evidence on a printer.
- Film recordings on such digital media as disc, USB stick, log files, tape or cartridge, and optical representation on either CD or DVD.

The investigator will endeavour to obtain as much original evidence as possible. In the event of a court appearance the court prefers the original evidence rather that a copy but will accept a duplicate if the original is lost or destroyed or is in the possession of a third party who cannot be subpoenaed.

9.7.5.1 Following the initial investigation and where considered appropriate, the investigator will report to/ liaise with the local Police and/or other external Agencies; this will only be done following consultation with the POL Head of security and POL Head of Information Security or substitute.

9.7.5.2 Copies of the initial and follow up reports will be submitted to relevant authorities and details of all investigations will be held on file by the POA Security to aid any subsequent trend analysis.

9.8 REMEDIAL ACTION

9.8.1 On Completion of report

When the final report of an investigation has been completed, it should be passed to the relevant authority for follow up action, the results of which should be referred back to the POA Security Manager.

9.8.2 Completion of Investigation

When an investigation is closed the POA Security Manager will ensure all details of the investigation have been recorded and can be made available for subsequent future analysis.

9.9 TRENDS & AUDITING

9.9.1 Frequency

POA Security Team carries out a monthly check of investigations and creates a summary report highlighting incidents to the POL Head of Information Security.

The report highlights trends or weaknesses which may need to be raised at future Information Security Management Forums (ISMF). POA will also submit a quarterly report to the Fujitsu Security Management Forum, to ensure that Fujitsu Security Incident trends can be reviewed in the round.

FUJ00080388

Appendix B Contacts

Security Incidents

- Jason Muir – GRO (POA Operational Security Manager)

Major Incident Manager Contact Details

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

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 should be contacted on the phone number detailed in the *Post Office Account Service Delivery Contact Details* on Share Point (see below) or on the date relevant POA OOH Duty Manager rota.

Outside these times, please contact the Major Incident 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.

POA Service Delivery Manager 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*.