Document Title:	POA Operations Incident Management Procedure
Document Ref:	SVM/SDM/PRO/0018
Release:	Not applicable
Abstract:	This document details the POA incident processes which supplements the incident processes defined in the Fujitsu EMEIA Business Management Systems Incident Procedure with the Post Office Limited specific requirements or requests.
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager
Author & Dept:	Matthew Hatch – POA Operations
Internal Distribution:	Steve Bansal, Matthew Hatch, Steve Evans, Andy Hemingway, , Sandie Bothick, Chris Harrison, Jerry Acton, Sonia Hussain, Piotr Nagajek, James Yates, Farzin Denbali & Chris Stevens
External Distribution:	See reviewer list; also distributed for information following Approval.
Information Classification:	See section 0.10

Approval Authorities:

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

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

0 Document Control

0.1 Table of Contents

0.2 Document History

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
0.1	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 Paula Hillsden	
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. 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)	

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
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.	
8.2	12-Sep-2017	Revised Appendix B, Contacts.	
9.0	12-Sep-2017	Approval version	
9.1	19-Oct-2018	Major re-write so that the Fujitsu EMEIA Incident Procedure is used as the primary process and this document maps those process requirements to specific POA teams, see flow diagrams. Also updated for TfSNow which replaces TSD. Amended section 9.5.2 to include breach of data protection legislation Amended section 0.5 Associated Documents removing withdrawn documents. Amended section 8.0 as SVM/SDM/SD/0001 has been superseded by SVM/SDM/SD/0007. Issued for formal POA Fujitsu review.	
9.2	28- Nov-2018	Amended sections 1.3, 2, 3.1, 4 and 4.2 for comments received.	
10.0	29-Jan-2019	Incorporated comments made by Steve Bansal and issued for approval Amendments made as part of Author review Removed the comment “Unavailability of sufficient tools for Incident diagnosis” from section 3.1 Risks	
10.1 DRAFT	22-July-2019	Added Splunk as a monitoring tool.	
10.2	24-March-2020	Updates in regards to only GDPR/PCI as a result of comments made by Bill Membery, following the AMEX SSK EPA file issue. Sections 6 Outputs, 7 Standards and 9.1 Scope	
10.3 DRAFT	20-April-2020	Following a Major Incident Management – Transition to Post Office Meeting held on the 15th April 2020, conducting a full review of the document in order to replace any reference to Atos with Post Office as of 1st May 2020. Reviewed the Author and Dept section, resulting in the removing of Tony Wicks and adding Kelly Nash.	

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		Following a review by Steve Bansal, the required changes have been made in-line with his comments. Will accept the changes and create Version 11.0	
11.0	18-June-2020	Reviewed by Sonia Hussain and minor changes have been made in line with her comments. Approved Version.	
11.1	14-July-2020	Added a minor change to section 9.5.2 Incident Categories, in relation to using the configuration items to indicate if there are GDPR, PCI or PCI and GDPR implications.	
12.0	15-Jul-2020	Approval version	
12.1	01-Sept-2020	Following a discussion with the GDPR team with reference to communication to the account about the configuration items related to PCI and GDPR added a new configuration item to TFSnow. This has resulted in section 9.5.2 category. No other changes have been added to this document other than what has been highlighted above.	
13.0	01-Sep-2020	Approval version	
13.1	08-Oct-2020	Amendment to section 9.5.2 Incident categories with reference to password protecting attachments internally and externally.	
13.2	21-Jan-2021	Made the amendments in line with the Steve Bansal's comments following a review. No other changes have been made to this document other than what has been highlighted above.	
14.0	21-Jan-2021	Approval version	
14.1	09-Apr-2021	Removed Kelly Nash from Author and Internal DL list. Removed Jason Muir and Bill Membery and added Geoff Baker to the Internal DL list and Optional Review from section 0.3. Review Details. Amendment to section 9.5.2 Incident categories with reference to sub-contractors i.e. Ingenico for Payment and Banking Service. Added Howard Booth to the Post Office Ltd Optional Review. Amended sections 0.6 Abbreviations and 0.7 Glossary with regards to KEL's and replaced with KB's. No other changes have been made to this document other than what has been highlighted above.	
14.2	27-May-2021	Amendments to section 9.5.2 Incident Categorises following feedback for Steve Bansal. Discussed with Phil Boardman with regards to CCN1672a Section 3.4.5 and Schedule I6 No other changes have been made to this document other than what has been highlighted above.	

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
15.0	05-July-2021	Approved version	
15.1	27-July-2021	Following the POA Improvement Incident and Problem meetings, added a new section 9.5.4 Horizon Defect Review (HDR) Configuration Items. Following a review of EBMS processes added the new section 9.5.5 Identification of what is a Security Incident Amended section 10.1.1Security Incidents to reflect Geoff Baker as the contact and not Jason Muir. No other changes have been made to this document other than what has been highlighted above.	
16.0	08-September-2021	Approved version No other changes have been made to this document other than what has been highlighted above.	
16.1	07-February-2023	Amended - P32 section 10.1.1 Security Incidents to reflect Farzin Denbali as the contact not Geoff Baker Section 5 Process Flows updated with the new links for EBMS Corrected spelling errors throughout. No other changes have been made to this document other than what has been highlighted above.	
16.2	23-February-2023	Accepted changes from 16.1. Also made changes in line with Steve Bansal's comments for 16.1. 10.1.3 OOH duty manager contacts details added. No other changes have been made to this document other than what has been highlighted above.	
17.0	24-February-2023	Approved version	
17.1	06-November-2023	Additional clarity on "Security Incidents" and corrections to text located in Appendix A	
17.2	09-November-2023	Horizon Defect Review (HDR) Configuration Items moved from Appendix A to the new section 4.3. Following a review Section 9 has been re-written with large parts being removed in order to reflect the current processes adhered to in line with the	

Version No.	Date	Summary of Changes and Reason for Issue	Associated Change - CP/PEAK/PPRR Reference
		EBMS processes. Enlarged the diagrams 5.1.5 Step 2 Trend Analysis and Reporting and 5.1.6 Step 3 Ownership Monitoring, Tracking and Communication. Additionally, Appendix B has been amended to add clarity to the contacts section. No other changes have been made to this document other than what has been highlighted above.	
17.3	15- January 2024	Accepted changes from version 17.2. Made changes in response to the feedback comments provided by Steve Evans. Section 0.8 Changes Expected updated. Notes for changes in version 17.2 updated. Also, section 0.4 Acceptance by Document Review has been updated to reflect Appendix A and the correct Document Section Heading. No other changes have been made to this document other than what has been highlighted above.	N/A
18.0	15-Jan-2024	Approval version	

0.3 Review Details

Review Comments by :	
Review Comments to :	Piotr Nagajek, Matthew Hatch and PostOfficeAccountDocumentManagement GRO
Mandatory Review	
Role	Name
POA Senior Service Director	Steve Bansal
POA MAC & OBC Team Manager	Sandie Bothick
POA Acceptance Manager	Steve Evans
POA Operational Security Manager	Farzin Denbali
Optional Review	
Role	Name
POA Infrastructure Operations Manager	Andy Hemingway
POA Business Continuity Manager	Sidharth Kumar
POA SDM Networks	Chris Harrison
POA SMC Manager	Jerry Acton
POA Defect & Quality Manager / Problem & Incident Lead	Matthew Hatch

POA Head of Online Services	Sonia Hussain
POA Service Delivery Manager	Piotr Nagajek
POA CISO and Management Consultant	Steve Browell
Post Office Ltd	
Post Office Ltd Security Manager	Dave M King <GRO>
Post Office Ltd POL Business Continuity Manager	Howard Booth <GRO>
Post Office Major Incident and Problem Lead, IT Service Operations	Paul I Smith <GRO>

Issued for Information	
Position/Role	**Name**
Post Office Ltd	
Post Office Ltd IT Document Specialist	Steven Vouthas <GRO>

(*) = 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	Appendix A	Security Incidents

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	PVCS
SVM/SDM/SD/0025			POA Problem Management Process	Dimensions
PA/PRO/001			Change Control Process	PVCS
SVM/SDM/SD/0007			Service Desk – Service Description	Dimensions
SVM/SDM/SD/0023			POA Incident Enquiry Matrix	Dimensions
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 BMS
			EMEIA Major Incident Management Process	EMEIA BMS

Reference	Version	Date	Title	Source
			EMEIA Root Cause Analysis (RCA) Process	EMEIA BMS
			Fujitsu Europe Security Policy Manual	EMEIA BMS
			Fujitsu Europe Security Incident Reporting Process	EMEIA BMS

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
BCP	Business Continuity Plan
BMS	Business Management System
HDI	Help Desk
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KB	Knowledge Base (in the context of this document, this is a workaround and diagnostic database) (These are also known as Knowledge Articles).
MAC/MAC Team	Major Account Controllers
OLA	Operational Level Agreement
OTI	Open Teleservice Interface
POA	Post Office Account
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
POL	Post Office Limited
SDM(s)	Service Delivery Manager(s)
SDU	Service Delivery Unit
SecOps	POA Security Operations team
SLT	Service Level Targets
SMC	Systems Management Centre
SSC	Software Support Centre
TfSNow	Triole for Services Now

0.7 Glossary

Term	Definition
KBs and KAs	Note that different support teams refer to knowledge database information as either Knowledge Articles or Known Base. Where within this document KB's 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 TfSNow 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 Information Classification

The author has assessed the information in this document for risk of disclosure and has assigned an information classification of FUJITSU RESTRICTED (COMMERCIAL IN CONFIDENCE).

1 Introduction

1.1 Purpose

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

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

1.2 Owner

The owner of the Incident Management process at the local POA level is the Fujitsu POA Senior Service Delivery Manager.

1.3 Objective

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 POL Service Desk are transferred/ referred from POA MAC / SMC to Post Office Service Desk.

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

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:

- 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

1.4 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).

Demonstrating a professional approach to, and Post Office Limited (the customer) and their clients.

1.5 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 Post Office 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.

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 Post Office 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
- 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.
- Splunk will monitor the Azure environment and will be used by the SMC to identify incidents from alerts. In the Full Azure Foundation Service Splunk will automatically raise incidents in TfSNow. It should be noted that these automatically raised incidents enter the process at step 1.2.3, and are not subject to prior steps in 1.1 & 1.2 of this process.

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 POL Service Desk. Mitigation is via e-mail.
- Non-availability of the OTI links to internal & external service desk tools. Mitigation is via e-mail.
- Lack of information given to the MAC / SMC regarding changes, 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 to investigate and resolve issues.
- Unavailability of sufficient tools for Incident diagnosis whereby manual diagnostics are unable to provide the same level of information as automated tooling.
- Non-availability of KEL or call management systems. Mitigation is a secondary SSC server for KELs and manual call processes.
- 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
  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.

4 Resources

The resources required for this process are:

- Process Owners
- Major Account Controllers team
- Service Management Team
- System Management Centre team
- Software Support Centre team
- Service Delivery Units
- TfSNow - Hosts Incident, Problem and Change databases
- Peak (third and fourth line incident database)
- ServiceNow and the HDI interface into TfSNow.
- OTI links
- TIVOLI (system components and event monitoring software)
- 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.
- Major Account Controller - To provide a single point of contact for Post Office Service Desk, dealing with the management of routine and non- routine Incidents, Problems and requests
- Incident Resolver - To accurately diagnose and resolve Incidents 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.

4.2 Incident Prioritisation within POA

The priority assigned to a TfSNow incident is either based on the priority documented in an existing KB or based upon the Urgency and Impact of the incident, refer to POA Incident Enquiry Matrix.

With the exceptions of Major Business Continuity Incidents and Major incidents POA generally utilise three priorities for incidents based upon the following guidelines.

Consideration must also be given to if the incident being reported is a Security Incident, if it is it must be notified to, and managed under, the POA Operational Security process (See Appendix A for guidance).

Priority 1 where there is an immediate impact to any live service or potential security incident requiring timely attention. Priority 1 incidents are voiced to a Support Delivery Unit, the POA Duty Manager and the Post Office Service Desk.

Priority 3 where there is an incident which has caused a loss of resilience, a failure or event which needs the timely attention of a Support Delivery Unit whose team will be voiced.

Priority 5 for other less urgent incidents.

Note1: Generally Priority 2 is used to align incidents with the customer Priority 2 incidents and Priority 4 incidents are not utilised within POA apart from CSPOA team. However, if there is a genuine business reason to do so incidents may be allotted at these priorities when it is consistent with EMEIA processes.

Note2: When incidents are transferred to the Software Support Centre (SSC) the TfSNow incident is transferred into a Peak incident system. Within Peak the incident priorities are defined as A, B, C and D. Therefore, when transferring TfSNow incidents into Peak ensure the following is adhered to:

TfSNow priority 1 equates to Peak priority A
TfSNow priority 2 equates to Peak priority B
TfSNow priority 3 equates to Peak priority C
TfSNow priorities 4 and 5 equates to Peak priority D

If this cannot be achieved through automation the MAC or SMC Agent undertaking the transfer is to log a comment on the TfSNow incident stating the TfSNow and Peak priorities.

4.3 Horizon Defect Review (HDR) Configuration Items

As a result, of the POA Improvements Incident and Problem Meetings new configuration items related to the Horizon Defect Review have been added to TfSNow, so that Incidents and Problems related to these types of defects can be reported against. The new configuration items that have been added are:

- HDR-EXP
- HDR-FIN
- HDR – OTHER

Once these have added to incidents and problems, reports or Dashboards in TfSNow can be created in order to aid in tracking such issues through to resolution and provide updates when requested.

Additionally, this will allow for reporting to be produced and provided to the customer with regards to incidents or problems that have had the HDR configuration item added, thus deeming there is a requirement to highlight them. These will be discussed in such forums as the Horizon Defect Review Forum

5 Process Flow

As stated in section 1.1 Purpose, this Post Office Account Incident Procedural document is solely to supplement the incident processes defined in the Fujitsu EMEIA Business Management Systems Incident Process. IRRELEVANT

Procedure: IRRELEVANT
IRRELEVANT

The following flowcharts provide an overview of the interactions for incidents with Post Office Account.

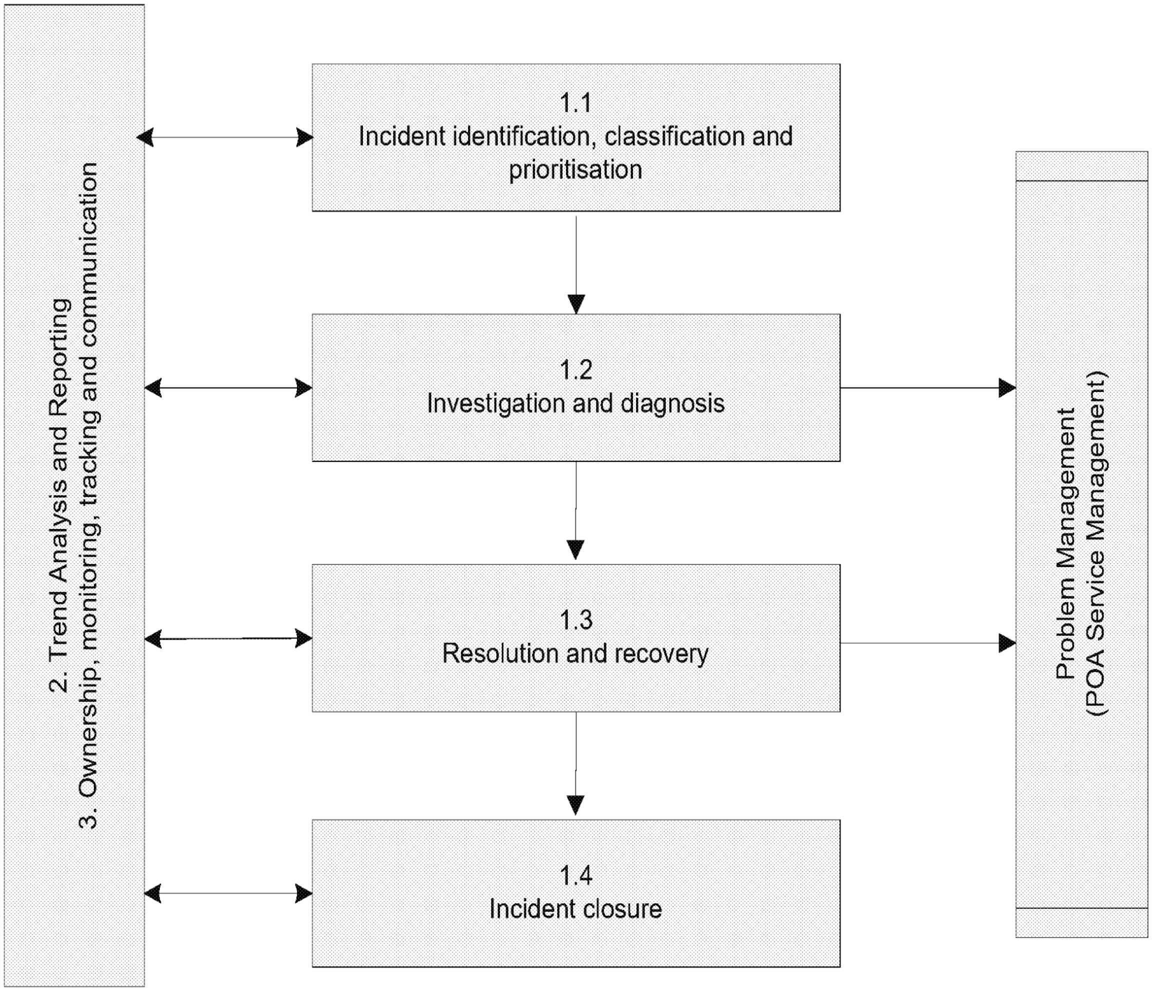

1.1
Incident identification, classification and prioritisation
1.2
Investigation and diagnosis
1.3
Resolution and recovery
1.4
Incident closure
2. Trend Analysis and Reporting
3. Ownership, monitoring, tracking and communication
Problem Management
(POA Service Management)

Figure 1: Level 1 Incident Management Process

5.1.1 Step 1.1: Incident identification, classification and prioritisation

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

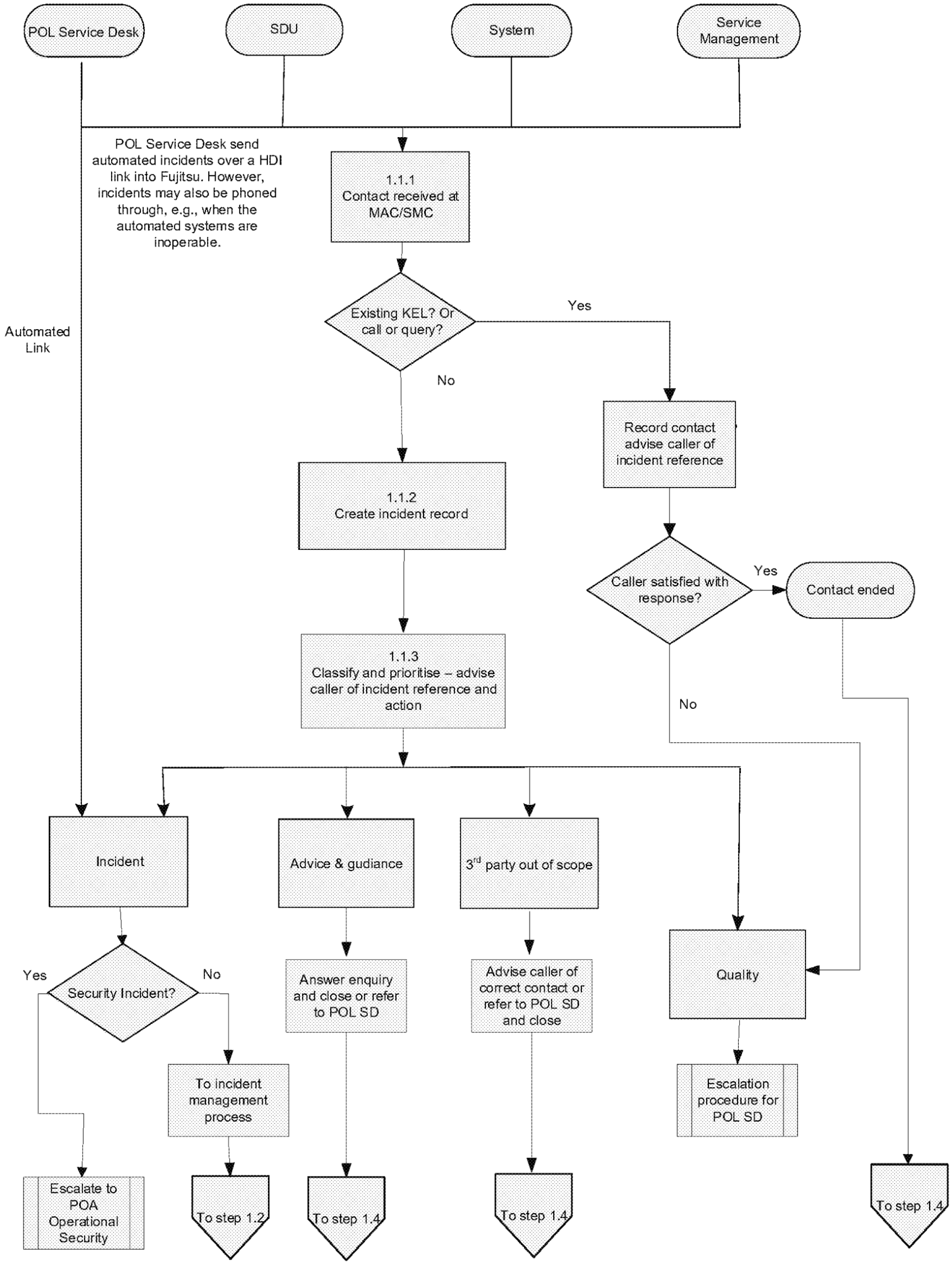

POL Service Desk
SDU
System
Service Management
POL Service Desk send automated incidents over a HDI link into Fujitsu. However, incidents may also be phoned through, e.g., when the automated systems are inoperable.
1.1.1 Contact received at MAC/SMC
Automated Link
Existing KEL? Or call or query?
Yes
No
Record contact advise caller of incident reference
1.1.2 Create incident record
Caller satisfied with response?
Yes
Contact ended
No
1.1.3 Classify and prioritise – advise caller of incident reference and action
Incident
Advice & gudiance
3rd party out of scope
Quality
Yes
Security Incident?
No
Answer enquiry and close or refer to POL SD
Advise caller of correct contact or refer to POL SD and close
Escalation procedure for POL SD
To incident management process
Escalate to POA Operational Security
To step 1.2
To step 1.4
To step 1.4
To step 1.4

Figure 2: Level 2 Incident Management Processes

5.1.2 Step 1.2: Investigation and Diagnosis

Responsible: MAC / SMC

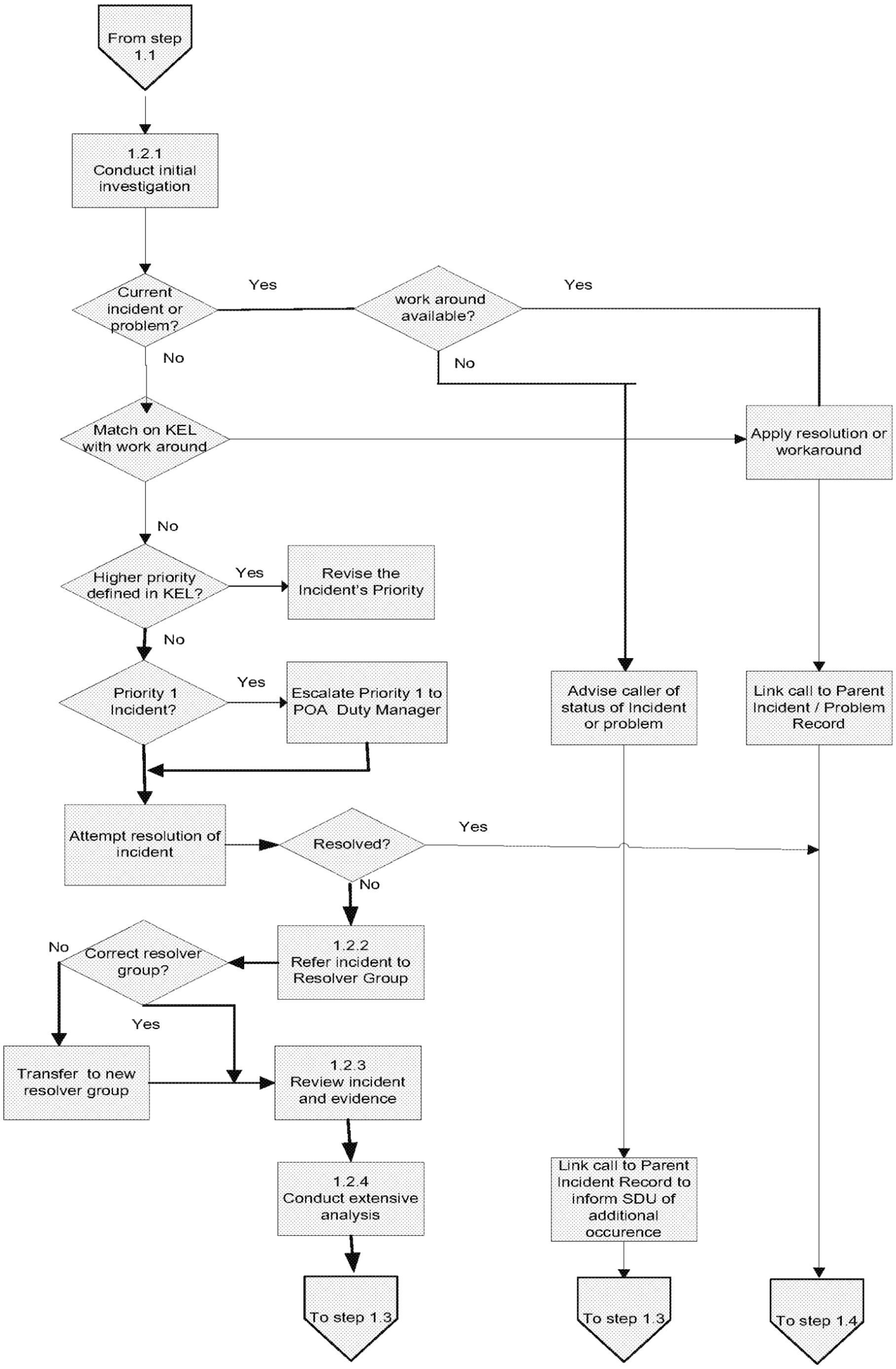

From step 1.1
1.2.1 Conduct initial investigation
Current incident or problem?
Yes
work around available?
Yes
No
No
Match on KEL with work around
Apply resolution or workaround
No
Higher priority defined in KEL?
Yes
Revise the Incident's Priority
No
Priority 1 Incident?
Yes
Escalate Priority 1 to POA Duty Manager
Advise caller of status of Incident or problem
Link call to Parent Incident / Problem Record
Attempt resolution of incident
Resolved?
Yes
No
No
Correct resolver group?
1.2.2 Refer incident to Resolver Group
Yes
Transfer to new resolver group
1.2.3 Review incident and evidence
1.2.4 Conduct extensive analysis
Link call to Parent Incident Record to inform SDU of additional occurence
To step 1.3
To step 1.3
To step 1.4

Figure 3: Investigation and Diagnosis

5.1.3 Step 1.3: Resolution and Recovery

Responsible: SDU's

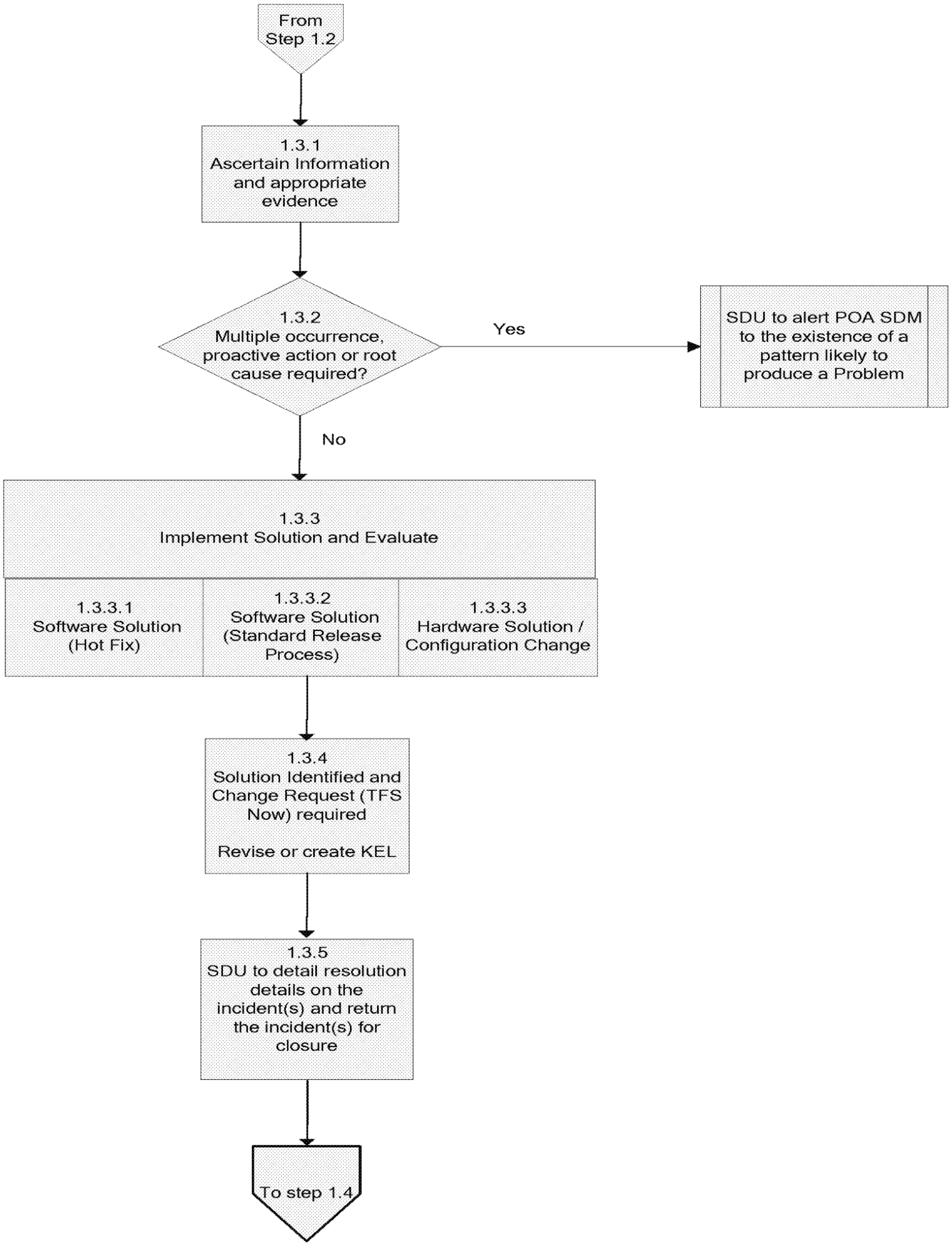

From Step 1.2
1.3.1 Ascertain Information and appropriate evidence
1.3.2 Multiple occurrence, proactive action or root cause required?
Yes
SDU to alert POA SDM to the existence of a pattern likely to produce a Problem
No
1.3.3 Implement Solution and Evaluate
1.3.3.1 Software Solution (Hot Fix)
1.3.3.2 Software Solution (Standard Release Process)
1.3.3.3 Hardware Solution / Configuration Change
1.3.4 Solution Identified and Change Request (TFS Now) required
Revise or create KEL
1.3.5 SDU to detail resolution details on the incident(s) and return the incident(s) for closure
To step 1.4

Figure 4: Resolution and Recovery

5.1.4 Step 1.4: Incident Closure

Responsible: MAC / SMC

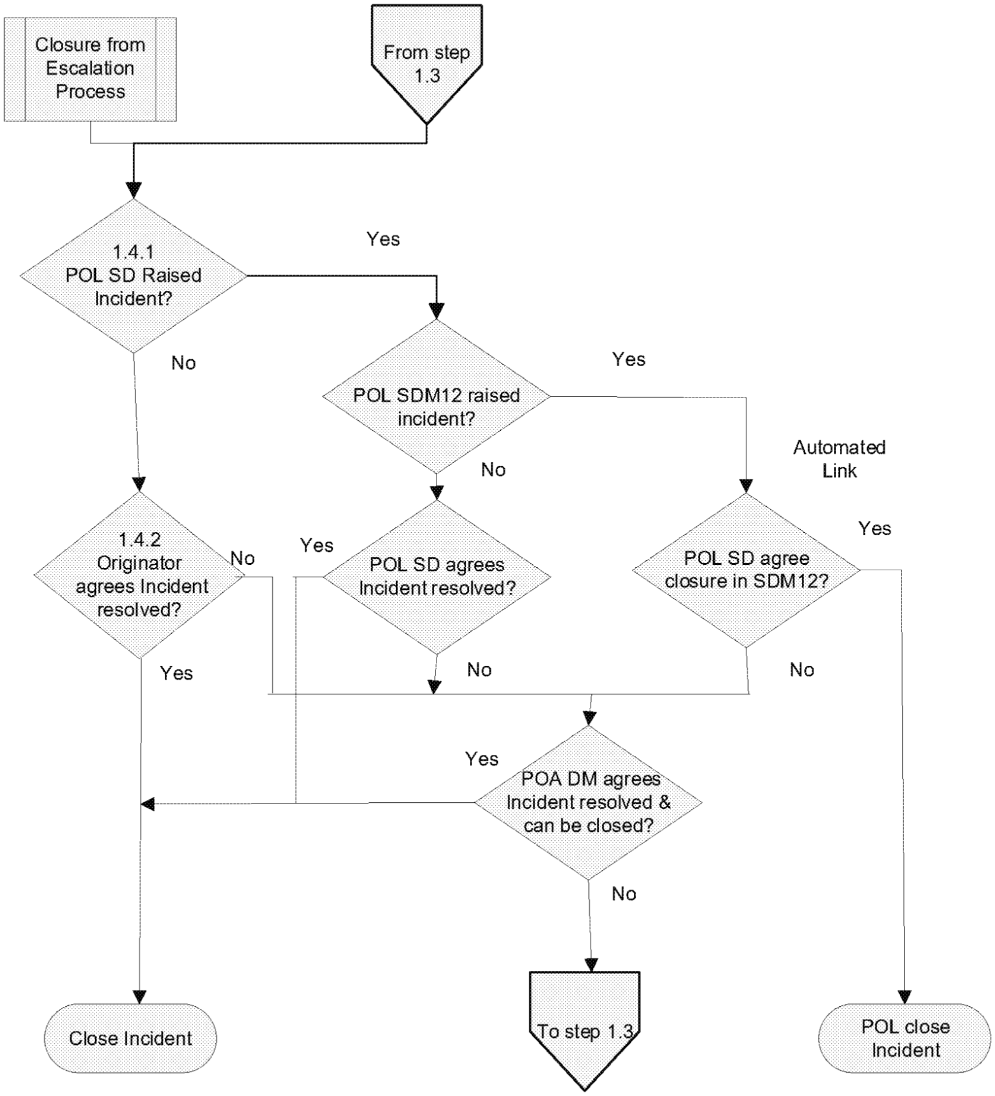
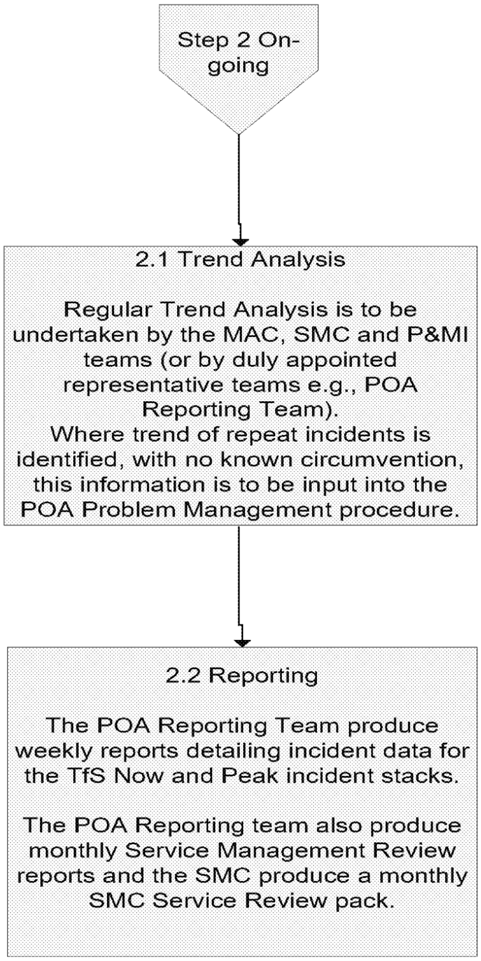

Closure from Escalation Process
From step 1.3
1.4.1 POL SD Raised Incident?
Yes
No
POL SDM12 raised incident?
Yes
No
Automated Link
1.4.2 Originator agrees Incident resolved?
No
Yes
POL SD agrees Incident resolved?
Yes
POL SD agree closure in SDM12?
Yes
No
No
Yes
POA DM agrees Incident resolved & can be closed?
Yes
No
Close Incident
To step 1.3
POL close Incident

Figure 5: Incident Closure

5.1.5 Step 2: Trend Analysis and Reporting

Responsible: Reporting Team, MAC / SMC, P&MI



Step 2 On-going

2.1 Trend Analysis

Regular Trend Analysis is to be undertaken by the MAC, SMC and P&MI teams (or by duly appointed representative teams e.g., POA Reporting Team).
Where trend of repeat incidents is identified, with no known circumvention, this information is to be input into the POA Problem Management procedure.

2.2 Reporting

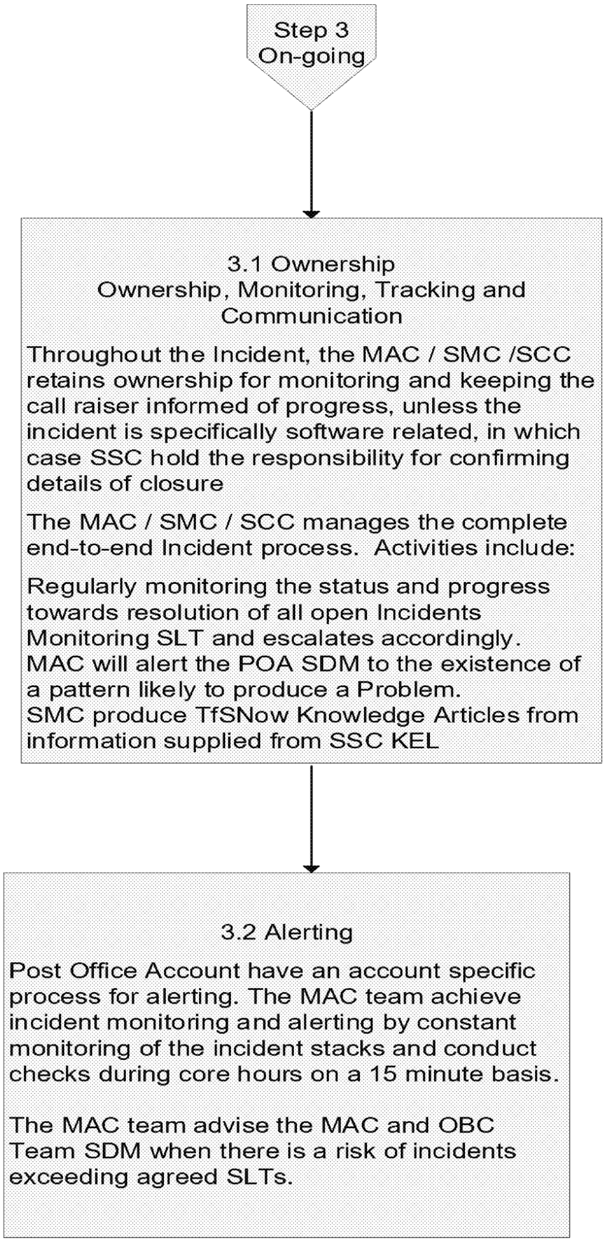
The POA Reporting Team produce weekly reports detailing incident data for the TfS Now and Peak incident stacks.

The POA Reporting team also produce monthly Service Management Review reports and the SMC produce a monthly SMC Service Review pack.

Figure 6: Trend Analysis and Reporting

5.1.6 Step 3: Ownership, Monitoring, Tracking and Communication

Responsible: MAC / SMC, SSC



3.1 Ownership
Ownership, Monitoring, Tracking and Communication

Throughout the Incident, the MAC / SMC /SCC 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 / SCC manages the complete end-to-end Incident process. Activities include:

Regularly monitoring the status and progress towards resolution of all open Incidents Monitoring SLT and escalates accordingly.
MAC will alert the POA SDM to the existence of a pattern likely to produce a Problem.
SMC produce TfSNow Knowledge Articles from information supplied from SSC KEL

3.2 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.

The MAC team advise the MAC and OBC Team SDM when there is a risk of incidents exceeding agreed SLTs.

Figure 7: Ownership, Monitoring, Tracking and Communication

6 Outputs

The outputs from this process are:

- Where one or more Incidents has been raised for a failure for which the underlying cause is unknown and a trend is identified, consideration shall be given to raising it as a Problem.
- An update to the Knowledge Base
- 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 – and specific to Security Incidents:

- Record in the SecOps Security Incident Portal for Security Incidents
- Notification to POL of Security Incidents
- Report on the status of Security Incidents as appropriate and in the monthly Information Security Management Forum (ISMF) report and at the POL monthly ISMF meetings.

7 Standards

This Process conforms to:

- ITIL Best Practice
- BS15000
- BS9001
- BS/ISO IEC 27001
- IEC 17799:2005
- PCI DSS version 1.2
- ISAE3402

8 Control Mechanisms

The contractual measures that apply to this service are described in the Service Management Service Description (SVM/SDM/SD/0007).

9 Appendix A: Security Incidents

As defined in the Fujitsu Europe Security Policy Manual requirements Section 16 (Security Incident Reporting):

> *A security incident is one or more events that may impact the confidentiality, integrity or availability of Fujitsu Europe assets and information, or those of our customers.*

All security Incidents (actual or perceived) within the Post Office Account ("POA") must be raised, investigated, and responded to.

Security Incidents are either:

- submitted on the POA SecOps Security Incident reporting form by POA team members via the reporting button on the POA portal (recommended and preferred option);
- emailed into the POA Security Operations (SecOps) mailbox by POA team members; or
- received via a TfSNow Incident being assigned to the POA SecOps assignment group.

In some cases this is supplemented by a phone call to the POA SecOps contact (see Appendix B).

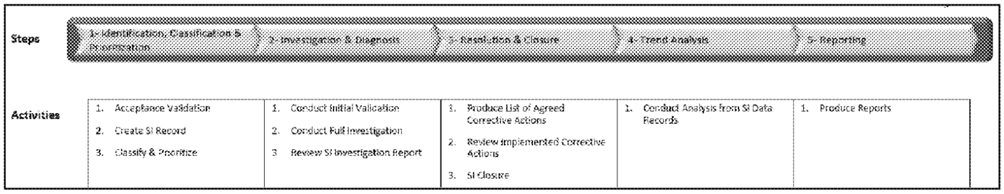
POA SecOps will raise Security Incidents with POL via the POL agreed process and will report on the status of Security Incidents as appropriate and in the monthly Information Security Management Forum (ISMF) report and at the POL monthly ISMF meetings.

POA SecOps log Security Incidents on the POA SecOps Security Incident portal where a complete record of the investigation and remediation actions will be held. An initial summary, and progress updates, may be added to any active TfSNow, if required, depending on the nature and sensitivity of the Incident.

ALL new and unique Security Incidents MUST also be reported into Fujitsu AskSecurity (Raise a Security Incident) and the AskSecurity Incident must be kept up to date. The AskSecurity reference should be added to any active TfSNow Incident.

Security Incidents are investigated by the POA SecOps team guided by the Fujitsu Europe Security Policy Manual requirements Section 16 (Security Incident Reporting) and in conjunction with required POA operational teams and Subject Matter Experts (SMEs).

POA SecOps use the Fujitsu Europe Business Management System – Security Incident Reporting Process and update the POA SecOps Security Incident portal. For quick reference, the 5 steps and activities are summarised here:



Steps	1- Identification, Classification & Prioritization	2- Investigation & Diagnosis	3- Resolution & Closure	4- Trend Analysis	5- Reporting
Activities	1. Acceptance Validation 2. Create SI Record 3. Classify & Prioritize	1. Conduct Initial Validation 2. Conduct Full Investigation 3 Review SI Investigation Report	1. Produce List of Agreed Corrective Actions 2. Review Implemented Corrective Actions 3. SI Closure	1. Conduct Analysis from SI Data Records	1. Produce Reports

Whenever a Security Incident is identified which presents a serious threat to conducting normal business, it must be contained and isolated as quickly as possible. POA SecOps will act with the required pace based on the specific severity of the Security Incident and will share and discuss any containment requirements with required POA operational teams and Subject Matter Experts (SMEs) and POL at the earliest opportunity.

Should it be considered necessary, the Security 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. The decision to take this action, and the required approach, would be discussed and agreed with POL in advance.

Cyber security threats come in many forms and the types of attacks are constantly changing. The vast majority of Security Incidents are minor. However, the severity and urgency of any threat would require specific consideration at the time.

A minor Security Incident will normally have limited and localised impact and be confined to one domain. For example:

- Accidental inclusion of sensitive information in an Incident in the service management toolset requiring redaction; or
- Accidental inclusion of sensitive information shared in an email requiring copies to be identified and deleted; or
- Files being sent to Fujitsu by third party suppliers that don't conform to the Application Interface Specification (e.g. unencrypted AMEX EPA files) resulting in GDPR\PCI data such as PAN numbers being shared unencrypted.

A more severe Security Incident presents a wider impact and level of concern. For example:

- An actual or attempted breach of the systems by a hacker; or
- The loss of customer data; or
- A breach of a legal data protection obligation; or
- The identified presence of malware in the environment (e.g. ransomware).

Severe Security Incidents would be declared as a Major Incident and managed following the POA Major Incident Process (SVM/SDM/PRO/0001).

10 Appendix B: Contacts

10.1 Security Incidents

10.1.1 Core Hours

- POA Security Operations Manager, or
- POA Security Governance Manager

10.1.2 Out of Hours

- Refer to the POA SecOps on-call rota

10.2 Major Incident Manager Contact Details

- Matthew Hatch – GRO
- Sandie Bothick – GRO
- Sonia Hussain - GRO
- Steve Bansal – GRO

10.3 Out of Hours Duty Manager Contact Details

Please refer to Account Call Out Rota for the applicable OOH Duty Manager

- Sandie Bothick – GRO
- Andy Hemingway – GRO
- Ramana Ravula – GRO
- Suseendran Narayanan - GRO
- Matthew Hatch – GRO

17.30 - 09.00 Monday PM to Thursday AM

17.00 - 09.00 Friday PM to Monday AM

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.

10.4 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.*