FUJ00080076

Document Title:	RMGA Customer Service Incident Management Process
Document Type:	Process Definition
Release:	*HNG-X / HNG-X Application Roll Out Transitional Period / Pre HNG-X Application Roll Out Transitional Period*
Abstract:	This document describes the Customer Service Incident Management Process
Document Status:	APPROVED This document contains sections that have been identified to POL as comprising evidence to support the assessment of named Acceptance Criteria by Document Review. These sections must not be changed without authority from the FS Acceptance Manager
Author & Dept:	Kirsty Gallacher – RMGA Service Support Manager
Internal Distribution:	Peter Thompson, Adam Parker, Mike Woolgar, Mike Stewart, Mik Peach, Ian Venables, Ian Mills, Peter Sewell
External Distribution:	Sue Lowther, POL Security Manager Gary Blackburn, POL Business Continuity Manager

Approval Authorities:

Name	Role	Signature	Date
Steve Denham	Fujitsu Services: RMGA Head of Service Management		
Michael Jacklin	HSD Operations Manager		

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

FUJ00080076

0 Document Control

0.1 Table of Contents

0 DOCUMENT CONTROL 2
0.1 Table of Contents 2
0.2 Document History 4
0.3 Review Details 4
0.4 Acceptance by Document Review 5
0.5 Associated Documents (Internal & External) 5
0.6 Abbreviations 6
0.7 Glossary 7
0.8 Changes Expected 7
0.9 Accuracy 7
0.10 Copyright 7

1 INTRODUCTION 8
1.1 Process Owner 8
1.2 Process Objective 8
1.3 Process Rationale 8

2 INPUTS 9

3 RISKS AND DEPENDENCIES 10
3.1 Risks 10
3.2 Dependencies 10

4 RESOURCES 11

5 PROCESS FLOW 12
5.1 Level 1 Incident Management Process 12
5.2 Level 2 Incident Management Processes 13
5.2.1 Step 1: Incident Detecting, Recording and Initial Classification 13
5.2.2 Step 2: Assign Priority and Initial Support 15
5.2.3 Steps 3/4: Investigation and Diagnosis; Resolution and Recovery 17
5.2.4 Step 5: Incident Closure 19
5.2.5 Step 6: Ownership, Monitoring, Tracking and Communication 20

6 OUTPUTS 21

7 STANDARDS 22

8 CONTROL MECHANISMS 23

FUJ00080076

9 APPENDIX A: SECURITY INCIDENT REPORTING 24

9.1 Scope 24
9.2 Aim 24
9.3 Changes 24
9.4 POL Incident Handling Guidance, ... 24
9.5 IT Incidents 24
9.5.1 Incident Definition 24
9.5.2 Incident Categories 24
9.5.3 Examples of IT Incidents 25
9.5.4 Containment 26
9.6 Reporting 26
9.7 Investigation 27
9.7.1 Policy 27
9.7.2 POL Security / Investigation Team 27
9.7.3 External Investigator 28
9.7.4 Evidence Rules 28
9.7.5 Process 29
9.8 REMEDIAL ACTION 29
9.8.1 On Completion of report 29
9.8.2 Completion of Investigation 30
9.8.3 UNIRAS Reporting 30
9.9 TRENDS & AUDITING 30
9.9.1 Frequency 30
9.10 Security Incident Process flow 31

FUJ00080076

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	

0.3 Review Details

Review Comments by :	30th June 2009
Review Comments to :	Kirsty Gallacher

Mandatory Review	
Role	Name
Fujitsu Services Fujitsu Royal Mail Group Account	
Head of Service Management	Steve Denham
HSD Operations Manager	Michael Jacklin
Optional Review	
Fujitsu Services Fujitsu Royal Mail Group Account	
CS Service Support Manager	Kirsty Gallacher

FUJ00080076

CS Operations Implementation Manager	Peter Thompson
CS Business Continuity Manager	Adam Parker *
CS Service Delivery Manager	Mike Woolgar
CS Service Delivery Manager	Ian Venables *
CS Service Delivery Manager	Mike Stewart
CS Service Delivery Manager	Ian Mills
CS System Support Centre Manager	Mik Peach *
CS Security Manager	Peter Sewell
SMC Operations Manager	Ian Cooley *
Post Office Ltd	
Security Manager	Sue Lowther*

(*) = 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)	1.0	13/6/06	Fujitsu Services Post Office Account HNG-X Document Template	Dimensions
CS/IFS/008			RMGA/POL Interface Agreement for the Problem Management Interface	PVCS
CS/PRD/021			RMGA Problem Management Process	PVCS
CS/PRO/110			RMGA Problem Management Database Procedures	PVCS
PA/PRO/001			Change Control Process	PVCS
CS/QMS/001			Customer Service Policy Manual	PVCS
SVM/SDM/SD/0001			Service Desk – Service Description	Dimensions
CS/FSP/002			Horizon System Helpdesk Call Enquiry Matrix and Incident	PVCS

FUJ00080076

Reference	Version	Date	Title	Source
			Prioritisation	
CS/REQ/025			Horizon HSD / SMC: Requirements Definition	PVCS
SVM/SDM/PRO/0001			RMGA Customer Service Major Incident Process	Dimensions
CS/PLA/015			HSD / SMC Business Continuity Plan	PVCS
SVM/SDM/SD/0002			Engineering Service Description	Dimensions
SVM/SDM/PLA/0031			Security Business Continuity Plan	Dimensions

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

0.6 Abbreviations

Abbreviation	Definition
A+G	Advice & Guidance
BCP	Business Continuity Plan
CISO	Chief Information Security Officer
CPP	Common Point of Purchase
FI	Forensic Investigator
HSD	Horizon Service Desk
ICR	Initial Case Report
IMT	Incident Management Team
ISO	International Standards Organisation
ITIL	Information Technology Infrastructure Library
KEDB	Known Error Database
KEL	Known Error Log (in the context of this document, this is a workaround and diagnostic database)
MSU	Management Support Unit
NBSC	Network Business Support Centre
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

FUJ00080076

Abbreviation	Definition
RFC	Request For Change
RMGA	Post Office Account
SAN	Storage Area Network
SDM(s)	Service Delivery Manager(s)
SDU	Service Delivery Unit
SLT	Service Level Targets
SMC	Systems Management Centre
SMT	Service Management Team
SRRC	Service Resilience & Recovery Catalogue
SSC	System Support Centre
TfS	Triole for Services
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.

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

FUJ00080076

1 Introduction

1.1 Process Owner

The owners of this process are the Fujitsu HSD / SMC Operations Manager and the RMGA Service Delivery Team Manager responsible for the Fujitsu contract.

1.2 Process Objective

The objective of this document is to define the process for Incident Management in the RMGA environment. 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 RMGA Information Security Policy (SVM/SEC/POL/0003).

This process applies to all Incidents raised by the RMGA HSD 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 RMGA HSD / SMC that should be placed with the NBSC are transferred/ referred from RMGA HSD / SMC to NBSC.

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

For clarity it should be noted that the HSD / IMT are responsible for managing/owning Incidents during business hours, with SMC assume this responsibility out of hours.

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).

This process takes account of the requirements of improved service to be delivered to POL, through the introduction of the HSD / SMC. The implementation of the IMT is documented and is aimed at delivering improved understanding and communication between POL and RMGA leading to an increase in the perceived service level within POL.

FUJ00080076

2 Inputs

The inputs to this process are:

- All Incidents reported by Contact with the HSD / SMC. Contact is defined as voice or Tivoli Alert as the methods of communication with the HSD / 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
  - Network Error
  - Logging via HNG-X web interface
- Severity and SLT information.
- Evidence of an Error.
- System Alerts received automatically from OMDB. Due to the urgent nature of these alerts they will be dealt with directly by SSC, with an update of workaround or resolution supplied to HSD / SMC. It should be noted that these alerts enter the process at step 3, and are not subject to steps 1 & 2 of this process.

FUJ00080076

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 HSD / SMC Incident Management System or HSD / SMC ONE systems. Mitigation is given in the HSD / SMC Business Continuity Plan.
- Non-availability of the OTI links to core & external service desk tools.
- Lack of information given to the HSD / 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
- Unavailability of sufficient tools for Incident diagnosis
- Non-availability of KEL or call management systems
- The provision of inadequate staff training within the HSD / 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 HSD / 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 (HSD / SMC ONE) kept up to date with POL business and services knowledge
- Fujitsu infrastructure support of the HSD / 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 ORFs, 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
- RMGA, SDU and 3rd party consistent co-operation in incident identification and resolution

FUJ00080076

4 Resources

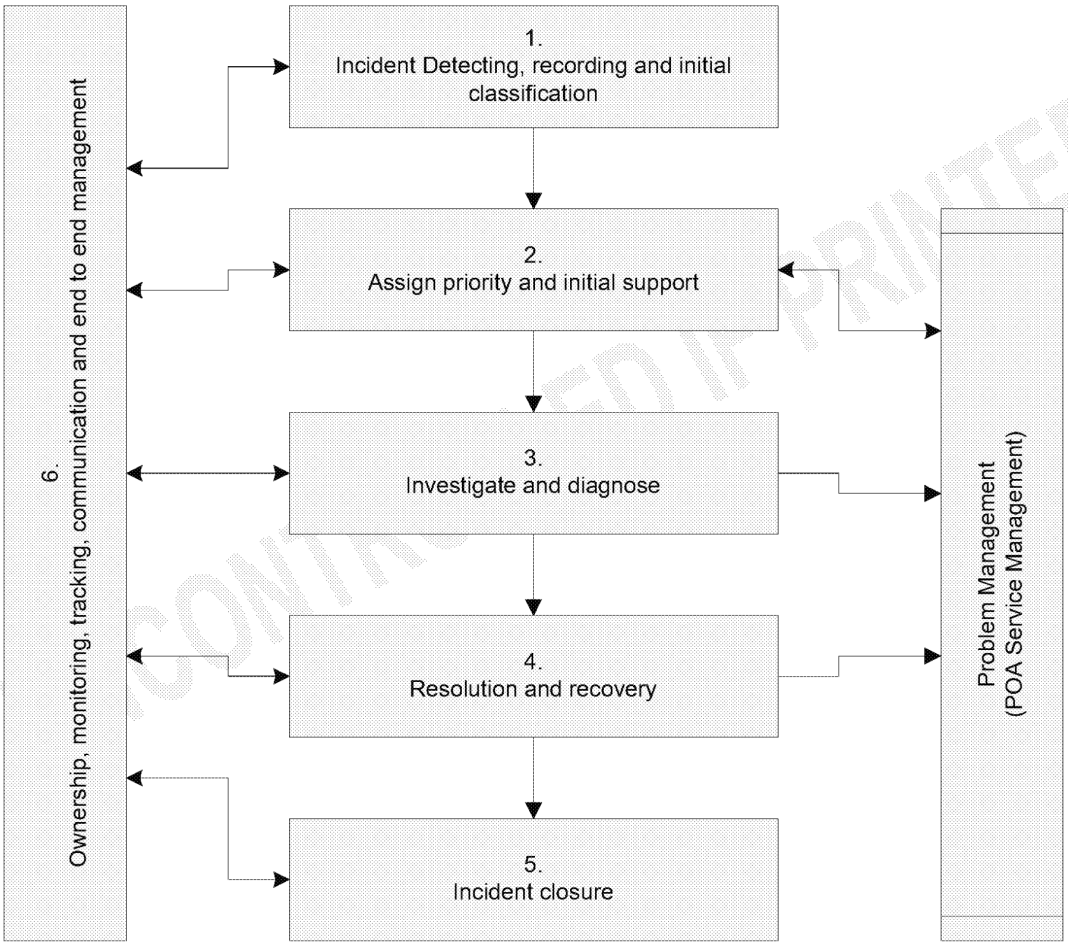
The resources required for this process are:

- Process Owners
- Incident Management Team
- Service Management Team
- HSD / SMC
- SSC
- SDU's
- Call Management System
- HSD / SMC ONE
- Peak
- Despatch 1
- TIVOLI
- Additional remote Management, Operational and Diagnostic tools
- Detailed Process and Procedure documentation

FUJ00080076

5 Process Flow

5.1 Level 1 Incident Management Process

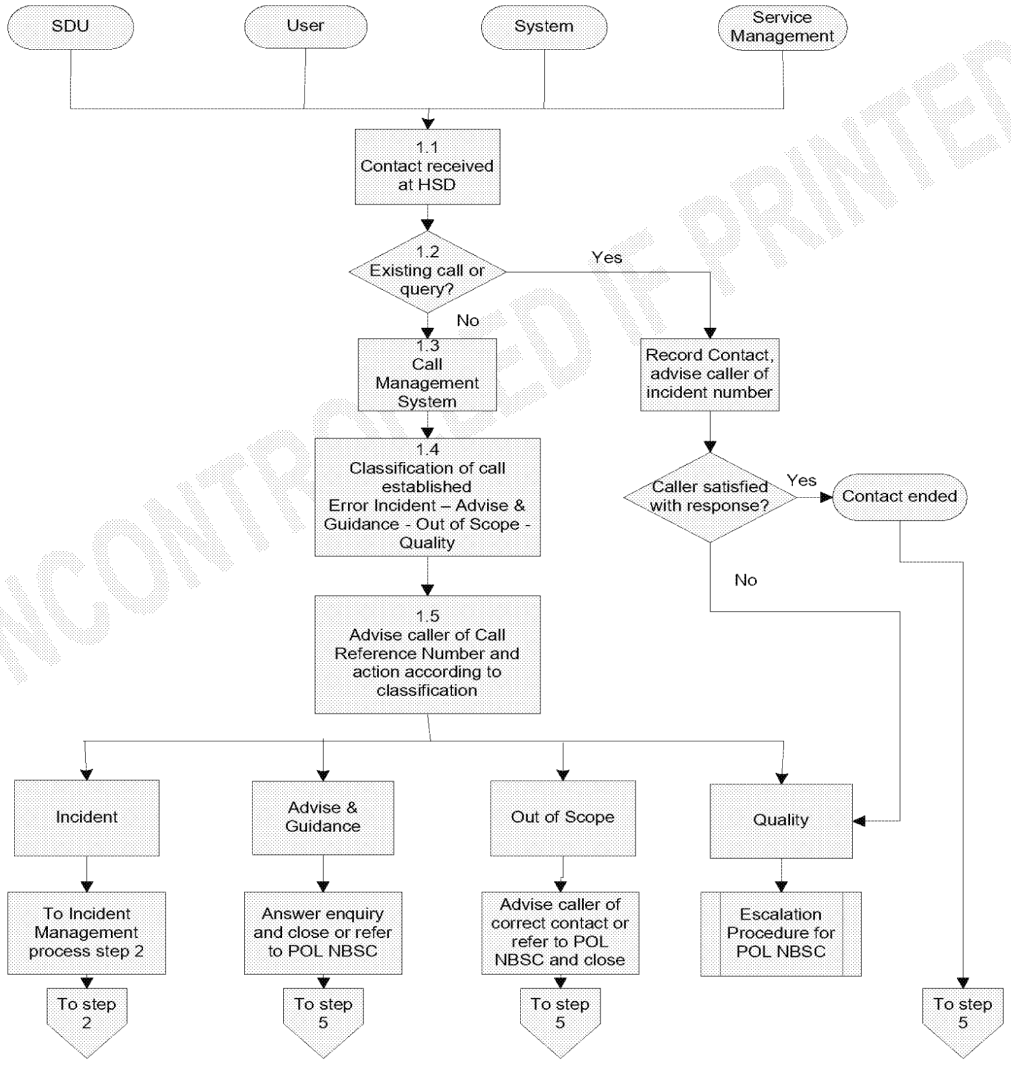


FUJ00080076

5.2 Level 2 Incident Management Processes

5.2.1 Step 1: Incident Detecting, Recording and Initial Classification

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



1.1 An Incident is received through contact (see definition in Section 2.0 above) with the HSD / SMC from:

- Users
- Fujitsu SDUs

FUJ00080076

- RMGA IT Service Management
- Third Parties
- Fujitsu Service Delivery Management
- Post Office Ltd, including POL Information Security

1.2 The caller may be enquiring about an existing Incident. Details are provided and if the response is satisfactory, contact is ended, moving the incident to step 5. 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 HSD / SMC alerts the relevant Service Delivery Manager to provide focused management of the Incident.

1.3 For a new Incident, Contact details are recorded if not system generated. 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
- Caller assessment of the priority of the incident.

1.4 Classification of Call determined as one of the following:

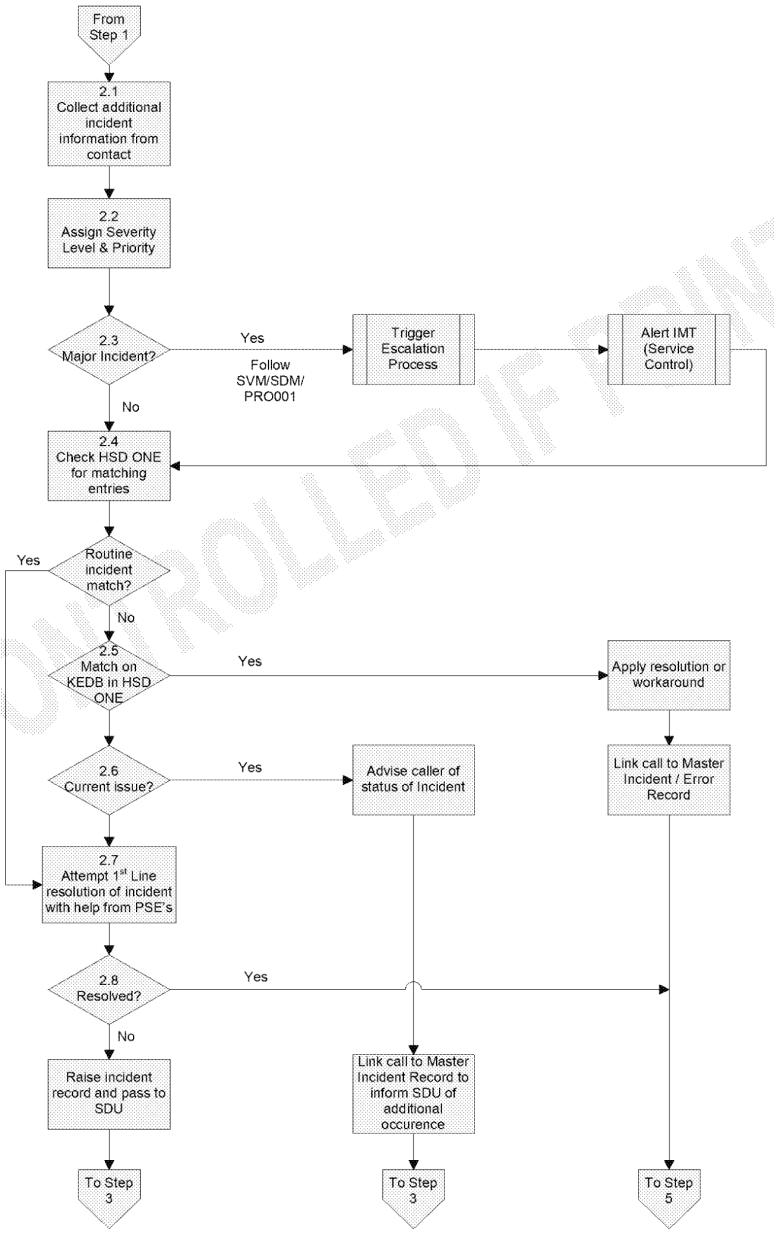
- Error Incident – invoke Incident Management Process Step 2
- Quality – record details of complaint or compliment and invoke the relevant Escalation Procedure.
- Advice & Guidance – Cold Transfer to NBSC.
- Out of scope – if the call is not within scope for the services provided by Fujitsu advise the caller of the correct number or refer to POL NBSC and close incident.

1.5 The caller is advised of call reference number and the incident follows the process as appropriate for the nature of the call

FUJ00080076

5.2.2 Step 2: Assign Priority and Initial Support

Responsible: HSD / SMC



2.1 The HSD / SMC agent collects additional information in order to determine the nature, impact and urgency of the Incident.

FUJ00080076

2.2 Call Severity is assigned based on the impact and urgency as per the criteria in the table below. Call Priority for Hardware and Network calls is assigned in accordance with the Priority matrix as detailed in Engineering Service Description (SVM/SDM/SD/0002), a copy of which each agent should have on their desk.

Severity	Importance	Definition
A	Critical	• BUSINESS STOPPED, a Post Office down, unable to process any business, or central system failure which will result in a number of Post Offices being unable to process work. • Forensic Investigation required following a compromise of card data.
B	Major	• BUSINESS RESTRICTED, a Post Office restricted in its ability to transact business, e.g. one counter down. • PCI Major Incident
C	Medium	• NON-CRITICAL, a Post Office working normally but with a known disability, e.g. an interim solution (workaround) has been provided. • PCI Minor Incident
D	Low	• INTERNAL, an internal HSH/HIT/SMC problem, e.g. a Service Desk PC or a phone set inoperable.

2.3 If the incident is considered a Major Incident as defined in SVM/SDM/PRO/0001 Major Incident Process, the Major Incident Procedures are invoked.

2.4 The HSD / SMC agent then attempts to resolve the Incident using the resources available. This starts by interrogating HSD / SMC ONE 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 HSD / SMC Support Matrix in HSD / SMC ONE.

2.5 If the Incident is not routine, the HSD / SMC agent checks for Known Errors listed in HSD / SMC ONE and the SSC KEL against records relating to the Incident symptoms. If a match is found, the agent informs the caller of the workaround or resolution available.

2.6 If there is no match in HSD / SMC ONE or the SSC KEL, the HSD / SMC Incident Management System stack is checked for current incidents outstanding. If a match is made, the caller is then advised of the status of the incident and the master record is updated to reflect the current occurrence.

2.7 If no match is made against the HSD / SMC Incident Management System stack, the HSD / SMC continues with first line resolution of the Incident assisted by the Product Support Engineers (PSE's). IMT are appraised of the position.

2.8 If the PSE's cannot resolve the Incident, it is referred to the relevant SDU using the HSD / SMC Support Matrix in HSD / SMC ONE. IMT are appraised of the position. For Hardware calls, the caller is given an indication of engineer arrival time, based on the SLA associated with the priority of the call.

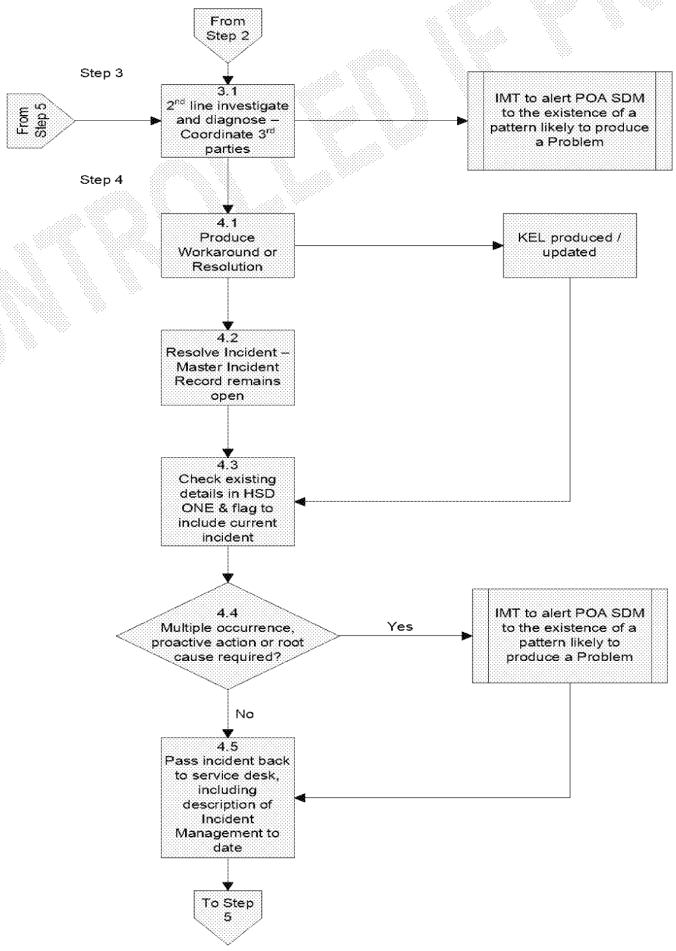
FUJ00080076

5.2.3 Steps 3/4: Investigation and Diagnosis; Resolution and Recovery

Responsible: SDU's

2nd line support stage. The referred SDU investigates and diagnoses the Incident, based on information already taken by the HSD / 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 IMT will alert the RMGA Service Delivery Manager to the existence of a pattern likely to produce a Problem.

Out of hours, SMC should check the OLA documentation to determine if out of hours support is available for the Service impacted. In the event that out of hours support is available, SMC will discuss incidents with the Duty Manager, who in turn will discuss incidents with the line of business SDM.



4.1 A workaround or resolution is produced by the SDU.

FUJ00080076

4.2 The SDU then either applies the workaround or resolution or passes it to the HSD / SMC to implement. The Master Incident Record (if one exists) remains open at this point.

4.3 The SDU checks the workaround or resolution has been successful. HSD / SMC are responsible for updating details recorded in HSD / SMC ONE, from details supplied via the KEL created by SSC. HSD / SMC ONE should be identical to SSC KEL in relation to Application Software, but may also contain additional information.

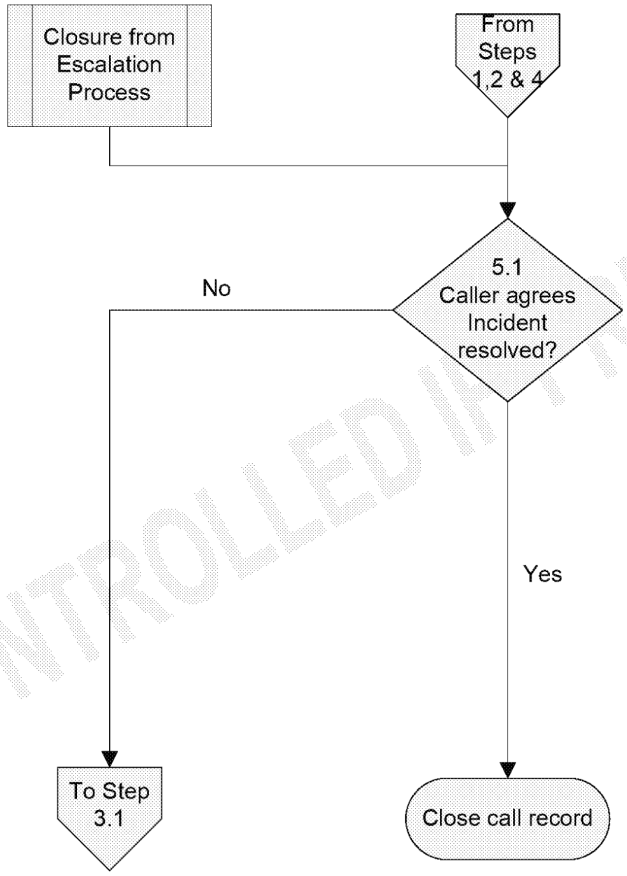
4.4 Where this Incident has a number of Calls referenced to it, or where there is a probability that proactive action is required to prevent further occurrences of this Incident the IMT will alert the RMGA SDM to the existence of a pattern likely to produce a Problem

4.5 The Incident is then passed to the HSD / SMC to manage the closure

FUJ00080076

5.2.4 Step 5: Incident Closure

Responsible: HSD / SMC



The Call is then closed with the agreement of the originator. If not, it will be returned to the SDU to be reworked.

FUJ00080076

5.2.5 Step 6: Ownership, Monitoring, Tracking and Communication

Responsible: HSD / SMC, SSC

Throughout the Incident, the HSD / 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 HSD / SMC manages the complete end-to-end Incident process.

Activities include:

- Regularly monitoring the status and progress towards resolution of all open Incidents
- Note Incidents that move between different specialist support groups, indicative of uncertainty and possibly a dispute between support staff
- 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, IMT will alert the RMGA SDM to the existence of a pattern likely to produce a Problem.
- Updating HSD / SMC ONE from information supplied from SSC KEL. This may be applied as a direct copy or amended for use by the agents, dependant upon the technical complexity of the update.

FUJ00080076

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 HSD / 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

FUJ00080076

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

FUJ00080076

8 Control Mechanisms

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

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

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

FUJ00080076

9 Appendix A: Security Incident Reporting

9.1 Scope

This annex outlines the process regarding the investigation, and reporting of all security incidents concerning the HORIZON Network and all IT equipment.

9.2 Aim

The aim of these instructions is to ensure that details of all IT related security incidents are reported to one central point and that any follow up investigations are managed in an efficient and auditable manner.

9.3 Changes

These work instructions are primarily for use by HORIZON Service Desk Staff, the RMGA Security Team, the POL Security Team, and SSC staff. Approval from POL is to be gained before any significant changes to the work instructions are implemented. All readers are encouraged to propose changes to Work Instructions, in writing, to the RMGA Security Manager.

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 guidelines. This document does not replace these, or, indeed, replace any part of the content - rather it lays down the RMGAccount framework under which the work is carried out.

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.

FUJ00080076

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):

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 RMGA Duty manager due to high volume of calls relating to the same type of incident it may well be a requirement to follow the RMGA Major Incident Process (SVM/SDM/PRO/0001) following the advice from the RMGA 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 RMGA 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 RMGA 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.

FUJ00080076

- Attacks on Fujitsu Services Post Office Account personnel via Information Systems. (I.e. Harassment, Duress
- Malicious/offensive/threatening/obscene emails.
- Obscene phone calls
- 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 examples, and by no means exhaustive. 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

9.6.1.1 Anyone reporting a security Incident should be encouraged to notify their Line Manager in the first instance. The Line Manager will gather as much detail of the incident as possible, following company procedures. He or she will undertake an initial local investigation into the incident, ensuring that in the case of missing equipment or materials that they have not just been misplaced. Information gathered will be entered into the initial case report template (ICR).

9.6.1.2 If the severity of the Incident is considered as Minor but warrants further investigation the Line Manager should immediately log a call with the Horizon Service Desk, stating that they are reporting a security incident, giving brief details. Please note that in certain cases there may be circumstances

FUJ00080076

where no details of a sensitive, nature should appear on the call log. Having logged the call and obtained a call reference number, the Line Manager may then continue with the investigation, and act as a liaison between the person reporting and all concerned parties. Once logged, the investigation will thereafter be referred to by the Call Number.

9.6.1.3 All Incidents reported to the Service Desk with a call reference and even when classified as Minor should still be forwarded to RMGA Security Management to determine if there is a Security Impact. 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

9.6.1.4 If the severity of the Incident is considered as Major the Incident details must be reported directly to the RMGA Security Manager immediately. Contact details are available on Café VIK. Depending on the type of Incident and the severity of the incident RMGA Security will make the decision to escalate the details to the POL Security. In the case of Data Centre incidents specifically Security will also inform the Data Centre Manager if this has not already been done. Regardless of the severity of the incident, when a compromise in card data occurs the incident must be reported to POL Security so that POL can comply with it's contractual obligations with it's card acquirer.

9.6.1.5 In all cases relevant details should only be recorded and discussed as necessary between the person investigating or Line Manager dealing with it and any relevant parties who need to be included in the investigation. Information on any incident must not be passed to anyone who is not directly involved with the investigation without the authority of RMGA Security Manager and the POL Head of Information Security.

9.6.1.6 Once a call is raised with the SSC the call will then be placed on the call stack of the RMGA Security Team, who will monitor the incident, assist or advise the Line Manager if required, and be available to take over the investigation should the need arise, but always be able to respond, within 2 hours of the initial call being made. (Minor Incidents (during normal working hours of between 9am and 5pm) and Major Incidents at all times.)

9.7 Investigation

9.7.1 Policy

Although all security incidents will initially be reported to the RMGA 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 RMGA 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 POL Security or the Investigation Team, all details of the investigation, and final outcome or reference details, should be recorded on the initial case report (ICR) and details will be recorded in the security Incident Log. 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.

FUJ00080076

9.7.2.2 In the event that the RMGA Security Manager takes ownership of an investigation, he will report the results to POL Head of Information Security and POL's Business Continuity Manager..

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

9.7.2.4 All initial investigations should be carried out at the earliest opportunity and any queries should be directed to RMGA 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 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 of 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

FUJ00080076

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 RMGA Security Manager or his nominated deputy. RMGA 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 they are:

- 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 RMGA 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 RMGA Security Manager.

FUJ00080076

9.8.2 Completion of Investigation

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

9.8.3 UNIRAS Reporting

On call closure, the RMGA Security Team will complete and notify UNIRAS where required. Thereafter the incident will be reviewed to identify the lessons learnt and the processes and relevant documentation will be updated as appropriate.

9.9 TRENDS & AUDITING

9.9.1 Frequency

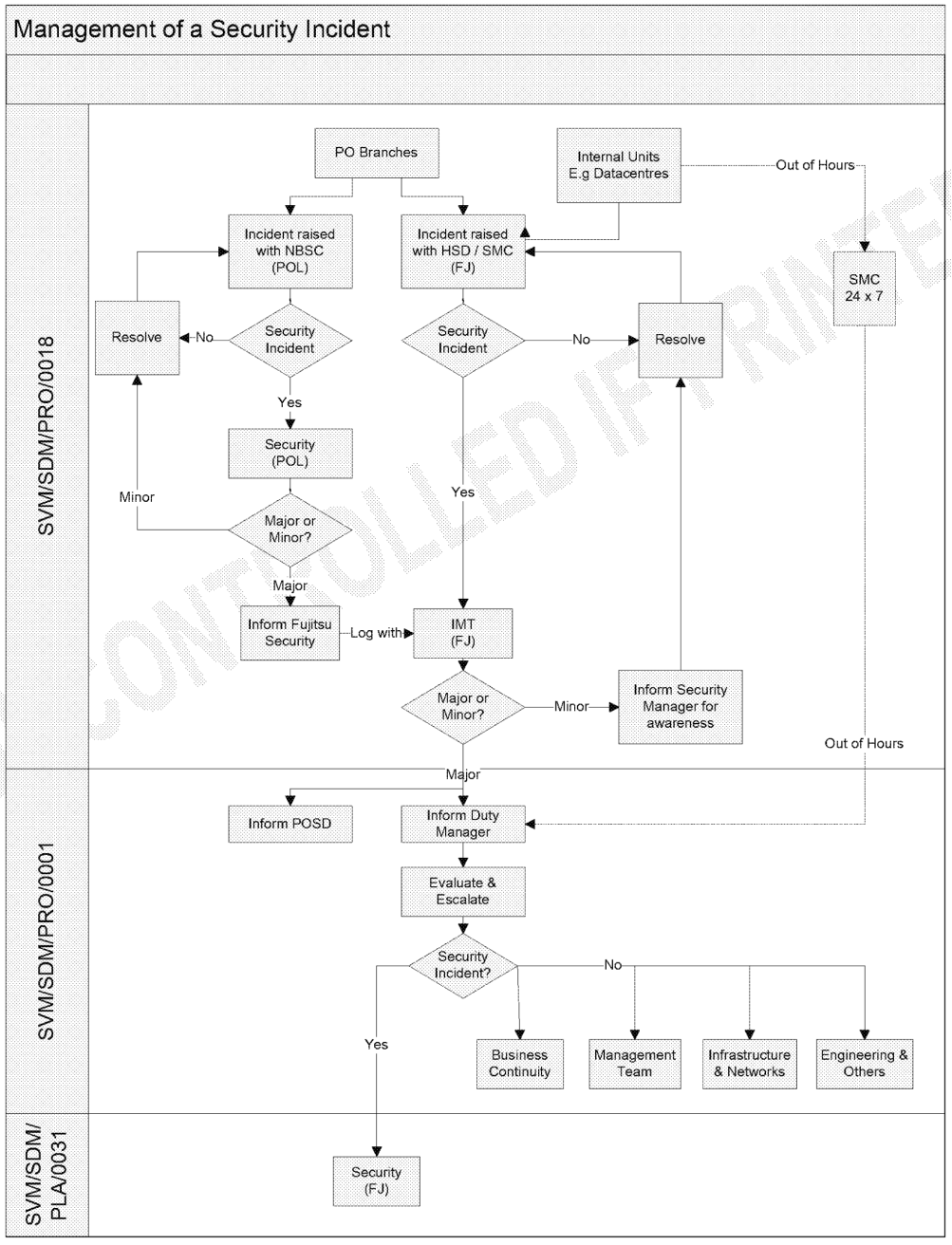
9.9.1.1 RMGA Security Team will carry out a monthly check of all investigations and create a summary report highlighting all incidents to the POL Head of Information Security.

9.9.1.2 The report will highlight any trends or weaknesses which may need to be raised at future Information Security Management Forums (ISMF).

9.9.1.3 Details from the monthly reports may also be considered suitable for Line Managers.

FUJ00080076

Appendix A Security Incident Process flow



FUJ00080076

Appendix B Security Incident Report Template

Identification						
Transition:				**Incident ID**		
Period:	**From:**		**To:**		**Reported:**	
Manager:					**Date:**	
Operational Security Report					**Overall Status:**	
Incident Details						
Further Action						
Lessons Learnt & Recommendations for Future Actions						