POL00398160

Post Office Limited
Incident Management Framework Document

Policy Owner – Antonio Jamasb
Process Owner – Rebecca Barker
Issue Number – Version 6.8
Issue Date – 15/08/2013

POL00398160

0. Document Control

0.1. Document Stakeholders

	Name	Role
Reviewers	Antonio Jamasb Gary Blackburn Andy J Jones Steve Beddoe Ivan Regan Rebecca Barker Ole Christensen Julie George Ian Trundell Duty Manager	Live Service & Continuity Manager Transition Manager Audit & Assurance Manager Senior IT Service Manager Security Project Manager Operations Specialist Security Programme Manager Head of Security Design Architect Live Service Desk
Document Sponser by	Steve Beddoe	Senior IT Service Manager
Policy Owner	Antonio Jamasb	Live Service & Continuity Manager
Document Author	Rebecca Barker	Operations Specialist

0.2. Document Version

Issue Number	Date	Comments/Summary of change
0.1	01.08.2002	First version of Crisis Management Team High Level procedures – base-lined document.
0.2	25.01.2005	Updated following an internal formal review of Crisis Management procedures within Post Office Ltd.
0.3	01.02.05	Updated following internal review comments.
0.4	24.02.05	Updated following formal review .
0.5	24.03.2005	Updated following internal review comments.
0.9	19.04.2005	Updated with additional contact details for PR Team.
1.0	10.05.2005	General Manager Service details added to BPT
1.1	06.09.2005	Updated changes to contact details
1.2	01.11.2005	Updated changes to contact details
1.3	13.12.2005	Updated with additional contact details for BPT Team.
1.4	21.12.2005	Updated with details of Blackberry users and contact details.
1.5	05.01.2006	Updated to incorporate and align flowchart to EBT protocol process.
1.6	12.01.2006	Reference to POL Business Continuity database included at appendix G.
1.7	13.01.2006	Updated changes to contact details
1.8	23.01.2006	Updated changes to contact details
1.9	23.02.2006	Updated changes to contact details
2.0	08/03/2006	Updated changes to contact details
2.1	10/03/2006	Updated changes to contact details
2.2	24/03/2006	Updated changes to contact details
2.3	06/04/2006	Document updated to take account of changes to structure in Operations Control.
2.4	12/04/2006	Updated changes to contact details
2.5	26/04/2006	Updated changes to contact details
2.6	30/01/07	Update new members of the Major Incident Escalation Group
2.7	21/03/07	Update new members of the Major Incident Escalation Group & business Protection Team
2.8	01/04/07	Update new members of the Major Incident Escalation Group &

POL00398160

		Business Protection Team
2.9	14/04/2008	Update contact details of the Business Protection Team and Blackberry Users
3.0	28/04/2008	Update contact details of the Business Protection Team
3.1	30/04/2008	Update contact details of the Major Incident Escalation Group
3.2	06/05/2008	Update members of the Major Incident Escalation Group
3.3	06/06/2008	Update contact details in Appendix A
3.4	11/08/2008	Change of name for Operations Control to Service Delivery. Update membership of Business Protection Team and Major Incident Escalation Group
3.5	24/02/2009	Added Telephone Conference call etiquette at Appendix I & new POL Payment Card Industry Major Incident Response Appendix J
3.6	23/04/2009	Added Home Telephone numbers of the BPT & MIEG. Added additional responsibility to both BPT & MIEG.
3.7	11/05/2009	Update changes of membership to BPT – Human Resources contacts
3.8	19/05/2009	Update contact details of BPT
3.9	01/06/09	Update contact details of BPT
4.0	20/07/09	Update MIEG and external contact details
4.1	21/09/09	Update external contact details
4.2	06/10/09	Update contact details
4.3	09/11/09	Update contacts of BPT and their contact details
4.4	04/01/2010	Update membership of BPT including contact details
4.5	08/02/2010	Added POL Director of Legal & Compliance & deputy to MIEG
4.6	10/02/2010	Re issued – housekeeping.
4.7	30/04/2010	Update membership of BPT , MIEG & Personal Secretary's
4.8	27/10/2010	Update membership of Major Incident Escalation Group & Business Protection team
4.9	16/11/2010	Update membership of Major Incident Escalation Group & Business Protection team. Update of PCI Incident Response Plan version 0.5 added as an embedded document
5.0	06/12/2010	Update membership of Major Incident Escalation Group & Business Protection team. Update of PCI Incident Response Plan version 0.52 Appendix M added POL's Out of Hours Service Desk First Escalation Point
5.1		Removed Lynn Hobbs from BPT & MIEG.
5.2		Updated membership of BPT & MIEG but not issued
5.3	26th July 2011	Updated contacts and details of the major suppliers to POL – appendix A. [Updated BPT membership] but not issued
5.4	4th October 2011	Replaced Debbie Moore HR Director in MIEG with Matthew Starks
5.5	21st November 2011	Replaced Gary Blackburn with Antonio Jamasb & removed HNG data centre migration process.
5.6	23rd November 2011	Replaced Hayley Fowell with Stuart Taylor on the BPT.
5.7	19th January 2012	Replaced David Gray with Chris Furmanski on the BPT Replaced Matthew Starks with Pauline Holroyd on MIEG
5.8	1st Feb 2012	Added Paul Meadows and Hugh Flemington to the BPT as Legal & Compliance's representatives.
5.9	12th March 2012	Replaced Mark Plant with Russell Hancock on BPT Added Sarah Munro & Michael A Brown to the BPT

POL00398160

		Added John Willcock to MIEG Removed Mike Young from MIEG
6.0	23rd July 2012	Removed all references to RMG Removed all RMG people from MIEG & BPT [David Simpson, Stuart Taylor & Shane O'Riordain] Added Jonathan Knox to the BPT Replaced Sarah Munro with John Willcock in BPT Added Ronan Kelleher & Ruth Barker to BPT Replaced Paul Meadows with Malcolm Staite
6.1	31st July 2012	Feedback following issue of version 62. Role changes/Directorate changes. New Communications director Added to MIEG
6.2	14th August 2012	Representatives of HR Directorate added to BPT
6.3	11th September 2012	Replaced Michael A Brown with Iain Gilbert as interim BPT member for Financial Services. Replaced Property representatives with Tim Wells and Cheryl Hurd. Replaced Richard J Barber with Mark Ward Added Sue Barton to MIEG new Strategy Director This version not issued.
6.4	14th November 2012	Replaced Mark Ward with Mark Pearce Removed Pauline Holroyd
6.5	24th January 2013	Replaced Ronan Kelleher with Sandra Mclaughlin in the BPT. Replaced Julian Tubbs with Dave Harcourt in the BPT Replaced Malcolm Staite with Nigel Tuppen in the BPT Replaced Malcolm Staite with Nigel Tuppen in the MIEG
6.6	12th April 2013	Added Blake Griffin Chief Technology Officer to BPT
6.7	5th August 2013	Replaced Nigel Tuppen with David Mason in BPT & MIEG
6.8	15th August 2013	Updated document with latest contact details
6.9	28th August 2013	Update document with feedback from PCI audit.

0.3. Feedback/Comments from the reviewers

Issue Number	Date sent	Audience document presented to	Comments/feedback provided
5.7	17/12/2012	POL Service Managers	Document digresses between Policy and Process, the document needs to be reviewed to establish what is a rule and what is a guideline. There is no mention of what is out of scope for Operational Change and no appendix sections with in the document.
6.2	05/05/2013	POL Service Managers	Documented to reviewed on a annual
6.9	28/08/13	Live Service Manager	PCI audit required complete overhaul of document. Document redrafted and renamed IMF Incident Management Framework. Submitted for formal sign off to version 7

POL00398160

0.4. Review and update

This document should be updated when any major change occurs. It will move to a new version number upon annual review and sign off. Appendix updates can occur as a draft version number update and needs not go out for formal signoff.

POL00398160

Contents

[TOC \o "1-3" \h \z \u]

POL00398160

1. Purpose

The purpose of this framework document is to explain how Post Office limited manages incidents within its domain and control, how its suppliers and clients operate Incident Management at a high level and their interactions with Post Office at a generic incident level.

Incident Management evoles during the incident lifecycle and this process document is a guide to support the process, rather than set immovable steps. The incident lead will decide whether the process steps are fit for purpose during any incident they own, should a new process step be used or a step deemed to be defunct, it will be reviewed during any Post Incident Review or washup and this document will be updated.

This document is a generic process document, Post Office will use individual process guides that will be recorded upon a call logging tool to manage specific incidents, where no individual process map has been developed the incident management team will fall back to using this document as a reference and guide.

The purpose of this document is to explain:

- roles and responsibilities in managing an incident and the methods by which management will be notified that a] an incident has occurred and b] that their involvement will be required
- the types of incidents likely to result in the invocation of Major Incident Management procedure
- the procedures that will be used by Post Office Ltd [POL] should a major incident occur.

2. Policy Statement

The goal of Incident Management is to provide the highest possible level of service availability through minimization of the impact of Incidents by:-
Having controls and processes in place.

- Ensuring all incidents are managed and logged within a single repository.
- Ensuring all incidents follow the same format.
- Delivering timely and effective communications.
- Delivering resolution timeframes acceptable to the business.
- Ensuring customer satisfaction maintained at all times.

The Post Office Ltd Incident Management process is owned and managed by the Live Service Continuity Team within Service Management.

Incidents can be managed directly by suppliers or clients if there is no significant impact to the Post Office critical service, financial arrangements, brand or reputation of Post Office ltd.

All service impacting incidents are managed using a three level management structure within Post Office Ltd. The involvement of each level is influenced by the severity of the incident.

Incident Management activities must be based on the established process and set of procedures which are referenced within

3. Incident Response

An evaluation of the extent and scope of the incident will be conducted by the Post Ofifce Service Desk, initially, with key business stakeholders to confirm if required, in order to help formulate an appropriate response plan. (Evaluations/updates can take place periodically, i.e. daily as incidents and the management of them evolve).

POL00398160

The answers to the following will help in that assessment (this list is not exhaustive and needs to be formulated for each type or incident):
Which systems are involved and to what extent? (How does this impact customer or business activities?)
How critical is each involved system?
What time of day/month/year etc.
Who are the customers of that service?
Should we invoke the InfoSecurity Incident Management Process?
Is there an ongoing threat?
Is there a need to invoke Business Continuity or Disaster Recovery to maintain or restore business services?
Are more monitoring and logging needed for the investigation?
Is it known if the incident has been perpetrated internally or externally of the business?
Does the business require additional resources, and/or external assistance (i.e. forensic investigators
Is the incident to be reported to the Police, Information Commissioner or Acquirer?
Is it likely the company will want to prosecute or take formal action against any perpetrator?
Any other information that will assist the decision making process.

Incident logging process is completed by Service Now which can be reached on the following URL:

[HYPERLINK "https://postofficeprod.service-now.com/"]

Instructions on how to use Service Now can be found in the Incident Logging Process document.

Should Service Now be unavailable a manual incident logging form can be found in Appendix 12 F

4. Incident Priority

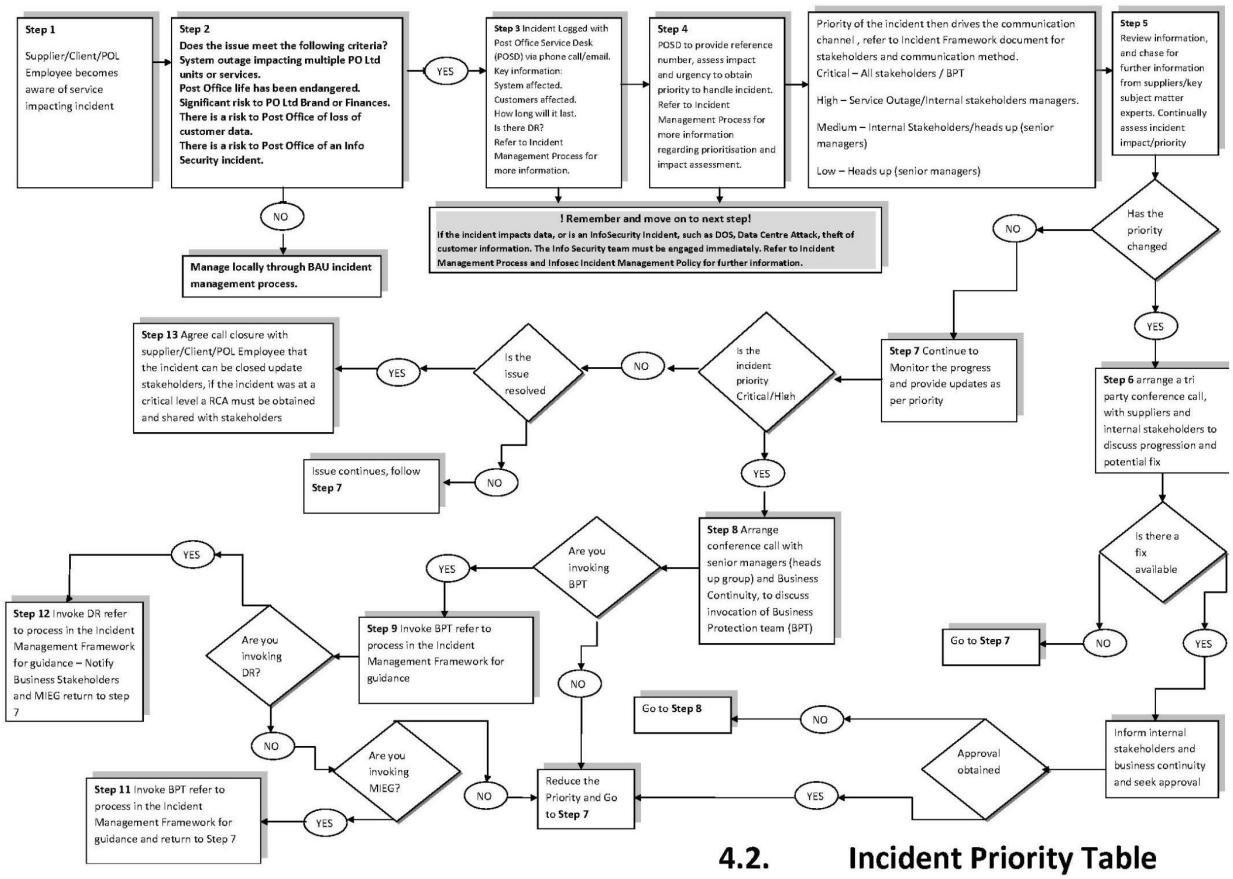
Incident Priority is a simple code assigned to incidents, problems and known errors, indicating the seriousness of their effect on the availability or Quality of Service. It is the means of assigning Severity for incident resolution.

The initial decision on an incident's severity rests with the Post Office Service Desk where incidents are normally first reported.
However anyone from within Post Office Ltd can call the Post Office Service Desk following and request that the BPT are engaged.

POL00398160

4.1. Incident Management Process

For more detail please see the Incident Management Process flow V0.1 which is attached within Appendix 13 G



4.2. Incident Priority Table

Below shows how the severity of an incident is assigned. Using Impact and Urgency. More detailed examples can be found within Appendix D

Severity Allocated	Impact		
Urgency	Very High	High	Medium
High	Priority 1	Priority 1	Priority 2
Medium	Priority 1	Priority 2	Priority 3
Low	Priority 2	Priority 3	Priority 4

4.3. Urgency Table

Urgency	
High	Is happening now, no immediate plan to restore.
Medium	Is happening now, but service will be restored shortly. Will happen within the next two days
Low	Could happen some time in the future.

POL00398160

4.4. Incident Impact Table

Impact	
Very High	Any failure that results in the total loss of a key service or an essential back end IT component. The Incident has an immediate and /or potentially prolonged adverse impact on one, some or all of the following: - Customer, Branch, clients, POL employees or POL brand and reputation.
High	Any failure that results in a partial loss of a key service, total loss of a non key service or back end IT component. Loss of customer data/information for over 50 customers.
Medium	Any failure that has the potential to become service, customer, or internal IT user affecting but can also be controlled and mitigated through effective management e.g. manual workarounds are in place. Loss of customer data/information for less than 50 customers
Low	Any failure that has no immediate impact or risk to services, customer experience, or the internal IT user community.

REMEMBER INCIDENT PRIORITY AND SEVERITY CAN CHANGE THROUGHOUT THE INCIDENT.

Further information can be found in appendix D

4.5. Incident Handling targets by Priority

Priority	Severity	Priority definition	Incident Logged within	1st Update within	Root Cause Analysis Produced
1	Critical	Any failure that results in the total loss of the service or an essential back end IT component. The Incident has an immediate and /or potentially prolonged adverse impact on one, some or all of the following: - Post Office Customer, Branch, clients, employees or POL brand and reputation	5 Minutes	30 minutes	Y
2	High	Any failure that results in a partial loss of the service, or back end IT component.	5 Minutes	1 hour	N
3	Medium	Any failure that has the potential to become service, customer, or internal IT user affecting but can also be controlled and mitigated through effective management e.g. manual workarounds are in place.	15 Minutes	6 hours	N

POL00398160

Priority	Severity	Priority definition	Incident Logged within	1st Update within	Root Cause Analysis Produced
4	Low	Any failure that has no immediate impact or risk to services, customer experience, or the internal IT user community.	30 Minutes	2 day	N
4	Low	Individual Issue or Service Update with minimal impact to the operational.	30 Minutes	2 day	N

The handling target time applies to standard Post Office working hours only: Monday – Friday, 09:00-17:00, excluding Bank Holidays and Post Office closure days.

4.6. Resolution Targets by Priority

Priority	Severity	Target Resolution Time	Resolution Target
1	Critical	1 day	90%
2	High	3 days	90%
3	Medium	5 days	90%
4	Low	8 days	90%

The resolution target time applies to standard Post Office working hours only: Monday – Friday, 09:00-17:00, excluding Bank Holidays and Post Office closure days.

4.7. Major Incident Definition

'An incident that has an immediate and/or potentially prolonged adverse impact on one, some or all of the following: PO Ltd Branches, POL employees, customers, clients or PO Ltd brand image'.

It is difficult to precisely define a Major Incident due to the number of variables that have to be considered as part of the impact assessment when an incident occurs. Such factors include time of day, business climate, day of week and time of year.

Major IT suppliers to PO Ltd – Fujitsu Services, HPES and CSC - are currently re-defining major incident trigger points. These will be included in future versions of this document to further assist in Major Incident definition.

A Major Incident is an incident that has occurred with a significant and potentially prolonged adverse impact on PO Ltd. The impact will be be significant to the Post Office Brand and Reputation. Typically these incidents will initially require a significant amount of reactive management before they can then be controlled and resolved.

To provide further guidance, a number of example scenarios together with the resulting business impact are now defined. The level of management input is also clarified.

More detail can be found within Appendix D

POL00398160

5. Incident Management Levels

There are three levels of management within PO Ltd who may be called upon to participate in the management of an incident.

5.1. Level 1 – Operational Support

PO Ltd Live Service Continuity team [Incident Leads]

All incidents and problems impacting live service within PO Ltd are reported into, controlled by and managed within this team.

If appropriate, this team will communicate to the PO Ltd Business Protection Team and the Major Incident Escalation Group to inform them of an incident and/or to request their input. [HYPERLINK \l "_Appendix_A_~"] includes the Service Management contacts.

PO Ltd Operational Support Functions [Subject Matter Experts]

Made up from operational teams across the Post Office Directorates. Key team members from Managed Services, Service Management, Network etc will be required in supporting actions needed to resolve an incident.

Supplier Technical Experts [Support Functions]

Made up from Supplier Technical Support teams such as Service Delivery Managers, Engineering Support, Network Support etc.

5.2. Level 2 - PO Ltd Business Protection Team[Business wide working group]

This team consists of empowered business representatives from across PO Ltd. These business area 'experts' are available at all times and will be used to support, inform and influence the management of a severity 1 & 2 incidents.

They are a decision making authority for Severity 1 & 2 incidents. BPT members are listed at [HYPERLINK \l "_Appendix_A_~"]. A detailed set of responsibilities is included at Appendix B[HYPERLINK \l "_Appendix_C"].

POL00398160

If required to participate or lead the management of a Severity 1 & 2 incidents, they will be contacted by SMS or telephone and provided with meeting details and a conference call number. The conference call will be operated as a Virtual Operations Room, see [HYPERLINK \l "_Appendix_E_~"]C.

5.3. Level 3 - Major Incident Escalation Group [Business Directors]

This group consists of Business Directors and some direct reports. They will be notified of all medium/high severity incidents via email from the PO Ltd Live Service Continuity team. If required to participate or lead the management of a Severity 1 incidents, they will be contacted by SMS or telephone and provided with meeting details and a conference call number. The conference call will be operated as a Virtual Operations Room, see [HYPERLINK \l "_Appendix_E_~"]C. The MIEG members are listed at [HYPERLINK \l "_MAJOR_INCIDENT_ESCALATION"].

6. Incident Management Communication procedures

Post Office during the lifecycle of an incident has many stakeholders that must be communicated with, using various mediums of communication.

Details and examples of incident communication can be found within Appendix E

6.1. Stakeholder Communication by Priority

Below details who and when teams and stakeholders should be communicated during the incident lifecycle.

Team or Stakeholder	Critical	High	Medium	Low
Business Protection Team (Senior Business Leads)	X	X	X	
Major Incident Escalation Group (Directors & Exco)	X			
Service Managers IT & Change	X	X	X	X
Communication Team	X			
Client Relationship Managers	X	X	X	X
Information Security Manager*	X	X	X	
Release, Change & Continuity Specialist	X			
Problem & Escalation Specialist	X	X	X	X
Senior IT Service Manager	X	X		
Business Continuity Manager	X	X		
Head of Information Security	X	X		
Head of Risk & Compliance	X	X		
Chief Information Officer	X			
Strategy Director	X			
Managing Director	X			
Branches	X	X		
Clients	X	X	X	

6.2. Communication type by Severity

Below details what forms of communication should be used dependant upon incident severity.

*This section is used as guidance to the types of communication means are available to communicate with various audiences.

POL00398160

Be aware during an Info Security Incident communications and engagement are critical. Always ensure that the subject matter experts within the Communications and Information Security teams are engaged for advice before any significant action is taken.

Severity	Email	Pageone	Phonecall	News Line	Smart Inform	MBS	Branch Email	Twitter
1	X	X	X	X	X	X	X	X
2	X	X	X	X		X		
3	X	X	X	X				
4	X		X					

7. Incident Management Roles and Responsibilities

A detailed set of responsibilities is included at [HYPERLINK \l "_Appendix_D"]B

This section is used as guidance for engagement with various audiences and stakeholders.

Be aware during an Info Security Incident communications and engagement are critical. Always ensure that the subject matter experts within the Communications and Information Security teams are engaged for advice before any significant action is taken.

7.1. Management Level 1 – Bronze Operational Support

Team or Stakeholder	Responsible	Accountable	Consulted	Informed
PO Ltd Live Service Continuity	X		X	X
PO Ltd Operational Support	X		X	X
Supplier Technical Experts	X		X	X
Business Protection Team				X
Major Incident Escalation Group				X
Service Managers IT & Change			X	X
Client Relationship Managers			X	X
Operational Specialist	X			X
Information Security Manager*	X		X	X
Release, Change & Continuity Specialist				X
Problem & Escalation Specialist				X
Live Service & Continuity Manager		X		
Senior IT Service Manager				X
Business Continuity Manager				X
Head of Information Security				X
Chief Information Officer				X
Director of Risk & Compliance				X
Managing Director				X

7.2. Management Level 2 – Silver Tactical Support

Team or Stakeholder	Responsible	Accountable	Consulted	Informed

POL00398160

PO Ltd Live Service Continuity	X			X
PO Ltd Operational Support				X
Supplier Technical Experts			X	X
Business Protection Team	X		X	X
Major Incident Escalation Group				X
Service Managers IT & Change			X	X
Client Relationship Managers			X	X
Operational Specialist	X		X	X
Information Security Manager*	X		X	X
Release, Change & Continuity Specialist				X
Problem & Escalation Specialist				X
Live Service & Continuity Manager	X		X	X
Senior IT Service Manager	X		X	X
Business Continuity Manager	X		X	X
Head of Information Security	X		X	X
Chief Information Officer		X		X
Director of Risk & Compliance				X
Managing Director				X

7.3. Management Level 3 – Gold Strategic Support

Team or Stakeholder	Responsible	Accountable	Consulted	Informed
PO Ltd Live Service Continuity			X	X
PO Ltd Operational Support				X
Supplier Technical Experts			X	X
Business Protection Team	X		X	X
Major Incident Escalation Group	X		X	X
Service Managers IT & Change				X
Client Relationship Managers				X
Operational Specialist				X
Information Security Manager*				X
Release, Change & Continuity Specialist				X
Problem & Escalation Specialist				X
Live Service & Continuity Manager	X			X
Senior IT Service Manager			X	X
Business Continuity Manager	X		X	X
Head of Information Security			X	X
Chief Information Officer	X		X	X
Director of Risk & Compliance	X		X	X
Managing Director		X	X	X

7.4. Invocation of Disaster Recovery

Team or Stakeholder	Responsible	Accountable	Consulted	Informed
PO Ltd Live Service Continuity				X
PO Ltd Operational Support				X
Supplier Technical Experts			X	X

POL00398160

Business Protection Team	X		X	X
Major Incident Escalation Group	X		X	X
Service Managers IT & Change				X
Client Relationship Managers				X
Operational Specialist				X
Information Security Manager*				X
Release, Change & Continuity Specialist				X
Problem & Escalation Specialist				X
Live Service & Continuity Manager	X			X
Senior IT Service Manager	X		X	X
Business Continuity Manager	X		X	X
Head of Information Security			X	X
Chief Information Officer	X		X	X
Director of Risk & Compliance	X		X	X
Managing Director		X	X	X

7.5. Incident Management Contacts & Availability

Below are the key contact points for Incident Management. For all contacts see Appendix A

Team	Email	Contact Number	Availability
Post Office Service Continuity Team	dutymanager GRO	GRO 1 Option	24/7 365 days a year
Business Protection Team	dutymanager GRO	1 Option	24/7 365 days a year
Major Incident Escalation Group	dutymanage GRO	1 Option	24/7 365 days a year
Post Office Change Control	GRO	1 Option	9-5 Monday to Friday excluding Bank Holidays
Post Office Problem Management	GRO		9-5 Monday to Friday excluding Bank Holidays

Post Office Service Continuity Team Management Escalation Structure, this should be used if a stakeholder, supplier or client do not believe the Service Continuity Team is managing an incident to the correct severity or timescales.

Escalation Level	Name	Role	Contact Number	Email
1	Rebecca Barker	Operations Specialist	GRO	GRO
2	Antonio Jamasb	Live Service Continuity Manager		
3	Steve Beddoe	Senior IT Service Manager		
4	Dave Hulbert	Supplier & Service Manager		
5	Lesley Sewell	CIO		

POL00398160

7.6. Post Incident Analysis

Once the response to the incident is complete and the business has returned to Business-As-Usual (BAU), the Incident Advisor shall convene a meeting with key parties of the incident to review what happened during the incident.

This can be done virtually for all low to medium incidents and recorded within the incident resolution, but for High & Critical a formal group should be convened.

The objective is to identify:
What did and did not work
The full impacts to the business
Any preventative measures and / or controls necessary to prevent a reoccurrence
Events and shortfalls against legal and regulatory requirements, corporate Policies and Procedures
Update policies and procedures as appropriate
Any staff training and awareness necessary to support future incident prevention or management.
Following this meeting any lessons learnt, or adjustments to any Policy documents are to be completed within two weeks, to ensure that the business is able to react / respond to any new events.
The Post Incident Review is to be documented, recorded and retained on file for a minimum of three years.

This information should be included upon the Post Office Post Incident Analysis document.

A template of this document is included within Appendix H

POL00398160

Appendix A ~ Contact details

BUSINESS PROTECTION TEAM ~ Key Members & Deputies **[Bold type** = primary contact for functional area]			
Email Name	**Directorate**	**Functional Area**	**Telephone**
Angela Van-Den-Bogerd	**Network & Sales**	**Head of Network Services**	GRO
Julia Marwood	Network & Sales	Head of Network Change & Improvement	
Mark X Gibson	Network & Sales	Senior Network Engagement Manager	
Tom Pegler	**Network & Sales**	**Crown Service & Efficiency Manager**	
Mike Granville	**Office of the MD**	Head of Stakeholder Strategy	
Manita Copper	Office of the MD	Stakeholder Relations Manager	
Paul M Brown	**Commercial**	**Head of Mails & Retail Services**	
TBC	Commercial		
John Willcock	**Financial Services**	**Head of Mortgage & Transaction Services**	
Iain Gilbert	Financial Services	Product Manager - Bill Payments	
Blake Griffin	**Strategy**	**Chief Technology Officer**	
Chris Furmanski	**Information**	**iT Governance & Strategy**	
Peter Stanley	**Strategy**	iT Design Authority Manager	
Keith Rann	**Network & Sales**	**Head of Supply Chain**	
Russell Hancock	**Network & Sales**	**Supply Chain - Senior Operations Manager**	
Dave Harcourt	Network & Sales	Snr Specialist Strategy - Supply Chain Operations	
Doug Brown	**Network & Sales**	**Supply Chain – Inventory & Planning**	
Clive Holmes	Network & Sales	Supply Chain – Inventory & Planning Manager - Retail	
Dave Hulbert	**Strategy**	**Service Management [Bridge to MIEG]**	
Steve Beddoe	**Strategy**	Service Management	
Antonio Jamasb	**Strategy**	**Service Management [Lead]**	
John M Scott	**HR & Corporate Services**	**Head of Security**	
Dave Pardoe	HR & Corporate Services	Senior Security Manager - Operations	
Julie George	**Strategy**	**Head of Information Security**	
Dave M King	**Strategy**	Information Security	
Cheryl Hurd	**Network & Sales**	**Area Facilities Manager**	
Tim Wells	Network & Sales	Portfolio Strategy Manager	

POL00398160

BUSINESS PROTECTION TEAM ~ Key Members & Deputies **[Bold type** = primary contact for functional area]			
Andy Garner	**Information**	**Senior Service Delivery Mgr Managed Services**	GRO
TBC	Information		
Rod Ismay	**Finance Services Centre**	**Head of Product & Branch Accounting**	
Alison Bolsover	Finance Services Centre	Branch Accounting Manager	
Alana Renner	**Communications**	**Deputy Communications Director**	
Richard Z Walden	Communications	Head of Corporate Communications	
Jonathan Knox	Communications	Channels Manager	
Sandra McLaughlin	Communications	Head of Press and Media	
Ruth X Barker	Communications	Senior PR Manager	
David Mason	**HR & Corporate Services**	**Head of Risk Governance**	
Hugh Flemington	HR & Corporate Services	Head of Legal	
Joe Connor	**HR & Corporate Services**	**Head of HR Services**	
Martyn P Lewis	HR & Corporate Services	Deployment Manager	
Fay Healey			
POL's OOH First Escalation Point Manager	**Strategy**	Service Management	See section 7.5 for Details

MAJOR INCIDENT ESCALATION GROUP ~ Board of Director Members and Deputies [**Bold** type = primary contact for functional area]			
Email Name	**Functional Area**	**Job Title**	**Telephone**
Paula Vennells	**Office of the Chief Executive**	**Chief Executive**	GRO
Mike Granville	Office of the Chief executive	Head of Shareholder Management	
Lesley J Sewell	**Information Directorate**	**Chief Information Officer**	
Deputy: TBC	Information Directorate	[Bridge to BPT]	
Martin Moran	**Commercial Directorate**	**Commercial Director**	
Deputy: Kevin Seller	Commercial Directorate	Head of Government Innovation Programme	
Nicholas Kennett	**Financial Services Directorate**	**Director Financial Services**	

POL00398160

Deputy: John Willcock	Financial Services Directorate	Head of Financial Services	GRO
Chris M Day	**Finance Directorate**	**Chief Financial Officer**	
Deputy: Stephen Hirst	Finance Directorate	Head of Finance Operations & Corp Services	
Mark R Davies	**Communications Directorate**	**Communications Director**	
Deputy: Alana Renner	Communications Directorate	Deputy Communications Director	
Kevin Gilliland	**Network & Sales Directorate**	**Network & Sales Director**	
Deputy: Neil Ennis	Network & Sales Directorate	Head of Network Transformation Programme	
Deputy: Roger W Gale	Network & Sales Directorate	General Manager Crown Sales	
Susan Crichton	**HR & Corporate Services**	**General Counsel**	
Deputy: David Mason	HR & Corporate Services	Head of Risk **Governance**	
Susan Barton	**Strategy Directorate**	**Strategy Director**	
Deputy: TBC	Strategy Directorate		

As a matter of course, the MIEG will also include the following people:			
Dave Hulbert	Information Directorate	Senior Service Manager	GRO

Post Office Ltd Service Management			
Name	**Functional Area**	**Job Title**	**Telephone**
Lesley J Sewell	iT and Change	Chief Information Officer	GRO
Dave Hulbert	Service Management	Senior Service Manager	
Andrew P Jacques	Service Management	Service Delivery Gateway Specialist	
Andy Garner	Service Delivery – Managed Services	Senior Service Delivery Manager – Managed Services	
Steve Beddoe	Service Management	Senior IT Services Manager	
Mark Weaver	Service Management	Senior iT Services Manager	
Antonio Jamasb	Service Management	Service Continuity Manager	
POL Service Continuity Desk [aka Duty Manager]	Service Management	Manned 24/7	

POL00398160

External Board of Director Equivalent Contacts			
Name	**Supplier Domain**	**Job Title**	**Telephone**
Rod Halstead	HPES	Managing Director, HPES UK Government	GRO
Andy Hunt	HPES	Operations Director , HPES UK Government	
Alexander Caviezel	JP Morgan	EMEA Region Executive	TBC
Stephen Long	Fujitsu Services	Director - Post Office Account	GRO
Mark Anstey	CSC	POL Account Manager	

External Contacts			
Name	**Supplier Domain**	**Job Title**	**Telephone**
James Davidson	Fujitsu Services	Operations Director POA Account	GRO
Adam Parker	Fujitsu Services	Business Continuity Manager	
Incident Management Team	Fujitsu Services	Incident Management of the Horizon Service	
Product Support 24/7	HPES	1st Line Support – 24 x7	
Mike Daley	HPES	Service Manager	
David Biggs	Santander	Business Contingency Manager	
Tommy Sussex	Santander	Senior Relationship Manager	
Jon Attwood	CSC	Service Management manager	
Moses Mclaughlin	HMS	Merchant Acquirer [auth Issues]	
Angela Halford	HMS	Merchant Acquirer[Auth Issues]	
Service Desk	LINK	LINK Duty Incident Manager	

POL00398160

8. Appendix B ~ Responsibilities

Business Protection Team

The Post Office Ltd Business Protection Team is made up of empowered representatives from key areas throughout the business. See the table at [HYPERLINK \l "_Appendix_A"] for details of the current Business Protection Team membership and additional useful contact points.

Responsibilities of members:

Be available and contactable on a 24x7 basis – business mobiles should be left switched on at all times except when on annual leave. They may be muted if required preferably on 'vibrate' mode as a minimum, but text/voicemail messages from the Live Service Continuity Team must be acted upon. These will appear in your message in box as being from 'DutyManager'.
Be the single contact point and co-ordinate all activities within your directorate/function.
Be responsible for making decisions on behalf of the business, and taking actions to quickly manage the adverse impacts of a major service incident.
Facilitate two-way communications between your directorate/function and the appointed working group– ensuring that where the incident impacts your directorate/function you have kept all interested parties within your directorate informed and continue to keep them informed on the progress of the incident through to resolution.
Ensure that members of the Live Service Continuity Team are informed/notified about any events in your area, which may lead to a major service incident.
Consider any communications that may be required following the post major incident review, and be instrumental in their Management, if appropriate to your directorate/function . For example, giving recognition if appropriate, sending out control reminders, etc.
Participate in periodic business continuity tests of the Major Incident Management procedures.
Notify the Live Service Continuity Team [email: duty manager GRO telephone GRO GRO if you leave the business, change roles, change directorates ,change contact details or wish to leave the BPT.

Responsibilities in the event of being assigned to the appointed Business Protection working group for a major incident:

Ensure consistent attendance throughout a major incident to ensure progress is not hindered. You should therefore make every conceivable effort to attend any meeting and/or conference call arranged. This may mean that pre-booked appointments have to be rescheduled.
Complete all actions assigned to you within the agreed timescales.
Wherever possible, take a second person to the working group meetings / conference calls. This will allow people to leave the meeting to seek additional information [if it is required during the meeting], without losing input from the directorate/function, or delaying the activities of the working group.
Participate in a post major incident review.
Consider any communications that may be required following the review, and be instrumental in their Management, if appropriate to your directorate/function . For example, giving recognition if appropriate, sending out control reminders, etc.

POL00398160

Major Incident Escalation Group responsibilities

The PO Ltd Major Incident Escalation Group is made up of PO Ltd Directors and some of their direct reports. See the table on [HYPERLINK \l "_MAJOR_INCIDENT_ESCALATION"] for details of the current Major Incident Escalation Group membership and additional useful contact points.

Responsibilities of members:

As per BPT plus:

Be contactable on a 24x7 basis – business mobiles should be left switched on at all times except when on annual leave. They may be muted if required, but text/voicemail messages from the Live Service continuity Team must be acted upon. These will appear in your message in box as being from 'DutyManager'.
Chair the Major Incident Escalation Group once invoked

POL00398160

9. Appendix C ~ Virtual Operations Room

Virtual Operations Room

In the event of a major incident the PO Ltd Live Service Continuity Team will immediately invoke the Virtual Operations Room [VOR].

The VOR will operate as a conference call facility and will remain open for the duration of the incident.Change can be continuously open/ or opened at set times.

The VOR will be chaired by the PO Ltd Live Service Continuity Team, or by a BPT member nominated by the PO Ltd Live Service Continuity Team, and will be the central point of contact to which members of the Business Protection Team report progress on assigned actions and information updates.

The VOR will also act as the conference call facility for strategic conferencing at specified times, as directed by the Chairperson. In the event of considerable information traffic flowing through the VOR then an alternative conference call facility would be employed for strategic forums, details provided via the VOR Chairperson.

Roles and Responsibilities

Chairperson

- Open VOR facility and chair facility for duration of the incident.
- Manage Incident and Decision Log for duration of the incident – this will be made up of the following headings:
    - Time of Contact
    - Contact From
    - Contact With
    - Notes of Discussion/Information
    - Decisions Made

Secretary

- Maintain Incident and Decision Log for duration of the incident as directed by Chairperson
- Advise Business Protection Team times of strategic conferences.

Business Protection Team

- On receipt of SMS log attendance at VOR with chairperson.
- Complete all actions assigned to you within the agreed timescales.
- Update the VOR [and the VOR only] on status of assigned actions.
- Feedback any information on incident/impact to the VOR [and the VOR only].
- Attend strategic conferences as directed by chairperson.
- Use the VOR for obtaining information

Conference Call Etiquette

In order for telephone conferences to run professionally the following etiquette is to be followed.

- The chairperson will set up and enter the conference call at least five minutes before its advertised start time and then start the conference call within five minutes of the advertised start time. Prior to commencement of the conference call the Chair will lock the call to late attendees [***7 Conference Lock and Unlock**]
- Upon joining the conference call the participant must state their full name and the directorate/team that they are representing.

POL00398160

- A roll call [#1] will be undertaken prior to the conference call starting by the note taker who will issue actions etc after the conference call to all participants.
- The chairperson will identify them self , host the call and set the scene/state the reason for the conference call.
- The conference call should be treated like any other meeting.
- If you can not attend the conference call then please let the chair know before the advertised start time , if possible.
- The conference call will aim to last no longer than 45 minutes.
- If possible arrange to be in a quiet room, away from the office or other disturbances to participate in the connference call.
- When participants are not speaking then they must mute their telephone handset – Participants can mute their line by pressing * then 6 to cut out any background noise when this is present. They can then unmute their line by pressing * then 6. This will reduce background noise on the conference call.
- If you are joining a conference call using your mobile phone, check before hand that you will be in a good signal reception area
- Be sure to keep your mobile phone a few feet away from your landline telephone handset as it can create a 'hum' when active.
- Take care not to rustle paper, type or make a noise that might disturb the call, unless your line is muted.
- Prior to speaking on the call the participant must state their full name.
- All participants on the call must observe common curtsey to other participants when they are speaking.
- At the end of the conference call, the chair will summarise the key actions and agree the next meeting date and time ,if relevant & thank everyone for their attendance and participation.
- The objective of the conference call is to resolve/manage the MBCI to a satisfactory conclusion.

Controlling a meeting

The meeting is easily controlled using the telephone keypad. Everyone has basic control over their own line while you, **as the Chairperson**, have an extended set of features.
Everyone can use...
***0 Signals the Co-ordinator for assistance** – available for help and advice.
***4 Equalises your volume automatically – adjusts the volume of your line.**
***6 Mutes / Un-mutes your phone line –** useful for noisy connections e.g. mobiles.

In addition, you as the Chairperson have access to:
#1 Conference Roll Call – play back name recordings to see who's dialled in.
#2 Conference Participant Count – tells you the number of attendees.
***2 Stop Audio Message –** stop any recorded messages e.g. Roll Call.
***7 Conference Lock and Unlock –** stop anyone, including the Co-ordinator,
gaining access to the meeting.
#9 Enable/Disable Chairperson Hang-up – allows participants to continue after the Chairperson has left.
End Conference – ejects everyone from the meeting.

Tip: Be sure to unlock a conference before requesting assistance using *0 as you will be unable to rejoin a locked conference.

Chairperson dial out

Call additional participants and ask them to join the meeting. You can call, speak in private and return to the meeting with or without the additional participant.#3 Initiates Chairperson Dial Out – the Chairperson gets a dial tone and is temporarily removed from the conference. Key

POL00398160

#3 and dial the telephone number. When the call is answered you can speak to them in private. Note – you must enter the entire telephone number including the STD code.
#4 Connect both parties to the conference – returns the Chairperson and new participant to the original conference.
#5 Connect Chairperson only to the conference – the Chairperson returns and disconnects the person dialled.
Tip: When you return to the phone conference with a participant, if name recording is set to on, there will be a small delay to them joining if they are prompted to record their name.

POL00398160

10.Appendix D – Incident Severity Examples

Below are example incidents to highlight how the severity of incidents can be set by the Post Office Live Service Continuity Team.

Title	Description	Impact	Urgency	Severity	Management Level
Transport Issue - Central London transport network security alert.	A major security alert on the tube network could during core business hours could have an immediate impact on our people in Administration sites, branches and the Supply Chain operation.	Depending on the scale of the incident, there could be post office branch closures, disruption to transport routes, exclusion zones, and difficulties getting to and from work. High Impact	Incident is happening now, action is required, but has potential to ease over time. High/Medium Urgency	1	MIEG [Level 3 Tactical Support]
Network Banking System - Electronic Benefits Transfer system failure during core business hours on a Monday.	EBT is the core banking sub-system provided by JP Morgan Electronic Financial Services Inc., which sits within the overall post office card account system infrastructure provided to Post Office Ltd by HP. The EBT system authorises post office card account withdrawals and holds core data for the post office card account.	A failure of the EBT system, or an issue that required EBT to be taken offline during core business hours would have a very high impact as it is a key Post Office product with an extremely large customer base. One of the key product areas. This failure would have political sensitivity and potentially long recovery times. High Impact	Immediate high profile business impact across the whole network because post office branches would not be able to perform card account transactions. High Urgency	1	MIEG [Level 3 Strategic Support]
Industrial Relations - Industrial Action in Supply Chain.	Industrial Action within Supply Chain would impact on the ability of Post Office Ltd to maintain the delivery and collection of cash to, potentially, all post office branches.	High Impact as all service could be affected. Could impact the Santander Giro Transactions which is a key Client.	Majority of Branches have sufficient cash holdings for short term issue. Cas Service also have robust contingency plans. Short term urgency Medium. Long term High	1/2	BPT [Level 2 Tactical Support]
Network Service Issue -	Talk Talk [Fujitsu's comms provider] use	So assuming approximately	An outage of a single cluster	2/3	LST [Level 1 Operational

POL00398160

Talk Talk Cluster Node failure.	Cluster Nodes in the Asymmetric Digital Subscriber Line [ADSL] network in providing primary comms links between Post Office Branches and the data centres. BT Wholesale also have around 90 cluster nodes and TalkTalk have around 65 cluster nodes.	11,000 PO primary network ADSL lines the average impact of a cluster node failure would be: • BTW cluster node = 30% of 11,000 / 90 = average impact 89 branches • TT cluster node = 70% of 11,000 / 65 = average impact 118 branches The cluster nodes are usually hosted at a BTW location and cover a local geographic area. Medium Impact	node during core business hours would result in an on-line service failure to all Branches connected to the failed cluster node for between one and three hours. This would be mitigated by the use of the in Branch wireless router where approximately 80% of the impacted Branches would automatically switch to the wireless Network Medium to Low Urgency		Support]
Application Issue - Automated Payment File Transfer Failure.	Automated Payment files detail payments made by customers at post office branches. The files are delivered overnight to clients by Fujitsu Services.	A failure in the delivery of the file[s] would have some impact on customers, post office branches and helplines, as clients will not have received details of AP payments. There could be some finansial penalties if files were not deliver. Med/Low	AP payments made by customers at post office branches the previous working day. This impact would be relatively low as it may take several days for customers & clients to have an issue. Low urgency	3/4	LST [Level 1 Operational Support]
Building Services Issue - Generator Failure at Future Walk, Chesterfield.	There would be a loss of resilience in the event of a power failure scenario at Future Walk.	A failure of the generator at Future Walk would have no immediate business impact. Low	Very low urgency as no impact to the initial operation or people. Low	4	LST [Level 1 Operational Support]
Information Security Issue - Payment Card Data Compromise at Data Centre.	Payment Card data (or Cardholder data) may include the 16 digit card account number, account name, expiry date,	A suspected compromise of this data at a data centre will invoke certain obligations on POL under	The affected data centre might not be reconnected until the investigation is complete which	1	MIEG [Level 3 Strategic Support]

POL00398160

	security code(s), amongst other information which may be stored on a payment card.	existing contracts with the Merchant Acquirer(s). Foremost is an investigation that which must include a complete forensic examination of all potentially affected systems and processes. This investigation is mandatory on POL. In order to complete their investigation the Forensic Examiners (FE) may require that the data centre be disconnected from all external networks and that affected systems be disconnected from all adjacent systems. High The investigation would also require a forensic copy be made of relevant data (process data, logs and audit records).	may take several weeks. There may also be significant financial penalties if POL are non-compliant to the Card Schemes security standard (PCI DSS) and/or if Cardholder data is found to be compromised. High		

POL00398160

11. Appendix E – Communication Examples and Details

11.1. Email – Start & End of Day Status Reports

Twice daily communication to a large and varied group of Post Office personnel about business affecting incidents. See key below which highlights the impact of the incident. We just other comments to mention issues that were not business impacting but we believe that the business needs to be aware of.

Branch Green
Web Green
Contact centre Green
Client Green
Colleague Green**Credence Reboot** – A late notification was received to confirm that CGI Logica experienced a high memory issue with web services and therefore had to re-boot Credence to resolve. Users may have experienced access issues between approximately 12:45 and 12:51. POLSD are currently investigating why we were not made aware before the incident occurred.
Other Comments: **Fujitsu Homephone & Broadband-** Fujitsu are unable to place call barring on customers homephone accounts, impact is low as not many customers require this function. This is currently being investigated by our supplier.

Key

Green – All related services available
Amber - A related service issues or ongoing limited client/customer impacting incident
Red - Ongoing significant Client/Customer impacting incident

POL00398160

11.2. Email – Incident Summary Reports

Incident summary report is used to collate information regarding the incident. It is a overview of the issues, steps taken and future steps this is usually used to send out updates to senior management.

Over 50s Web Issue - Q17882989 SR1869648B

Issue
It was identified by POL that there was an issue when trying to complete the Over 50s journey on the web. At the last stage of the journey, an error message was encountered.

Impact
Investigations highlighted that there have been no successful purchases on the web since the product the product was relaunched on 07 November 2012 following changes to the product.

Root Cause
The cause is still under investigation, but appears to be related to a firewall issue between Aviva and Capgemini.

Actions taken to Date

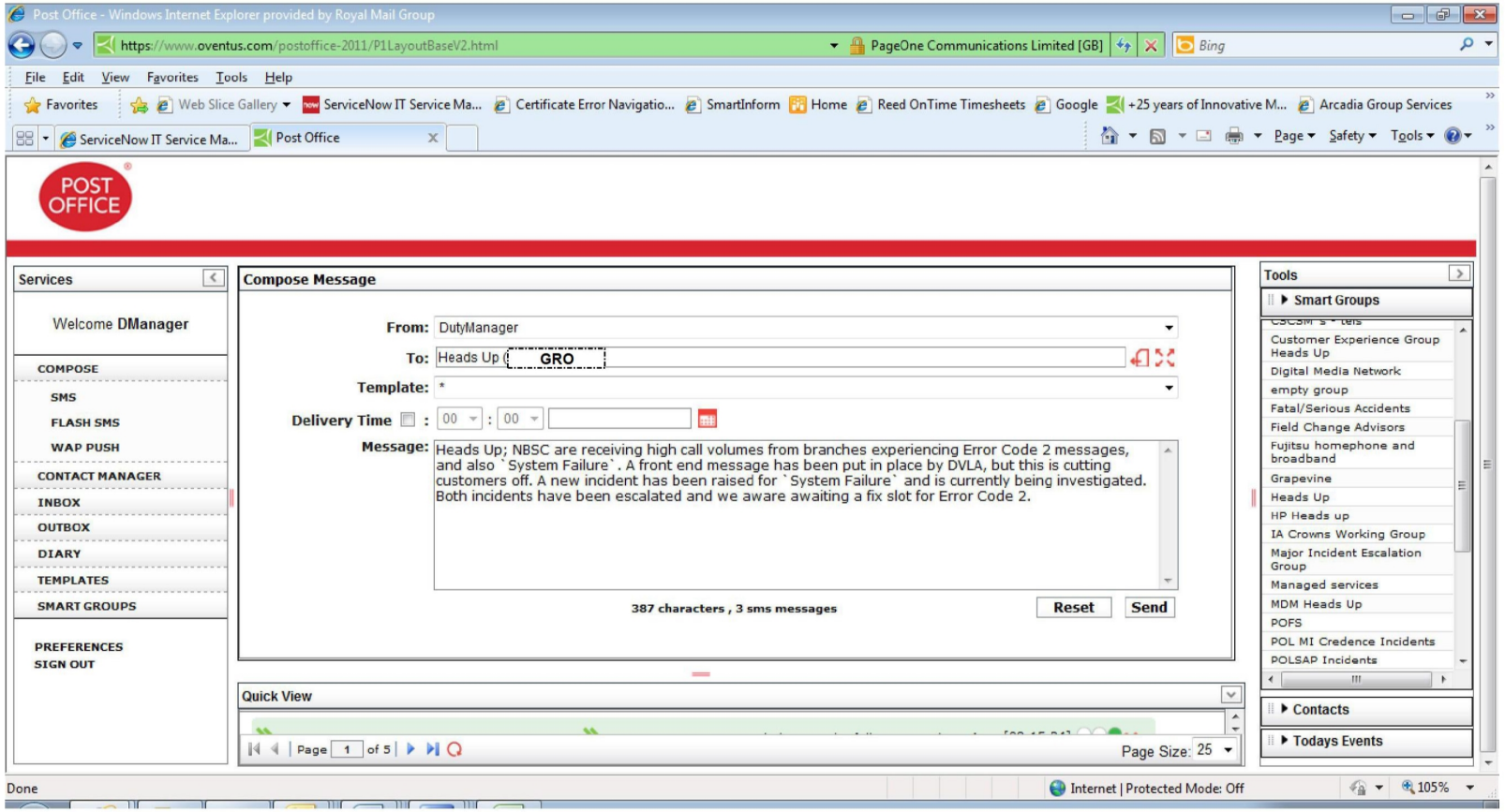
- 31 Jan 2013 - Conference call held with suppliers to progress the incident and facilitate communications between Aviva and Capgemini.
- Multiple investigations into firewalls in both Capgemini and Aviva domains, including information share between the two, with certain technical elements being able to be eliminated.
- Escalation within Aviva domain.
- 07 Feb 2013 – Conference call held with suppliers, again, to progress actions required for resolution. Agreed outputs

Next Steps
Agreed outputs from today's call include Capgemini to find out if traffic is hitting Aviva's Platform and provide evidence of this, and Capgemini to perform a test transaction in a test environment and if successful make comparisons with the Live Over 50s Journey.
A further conference call is scheduled for 08 Feb 2013.
A daily conference call will be convened until POL has a high level of confidence that a robust action plan is in place to enable swift resolution.

POL00398160

11.3. Pageone SMS Text – Incident Notification, Update and Resolution

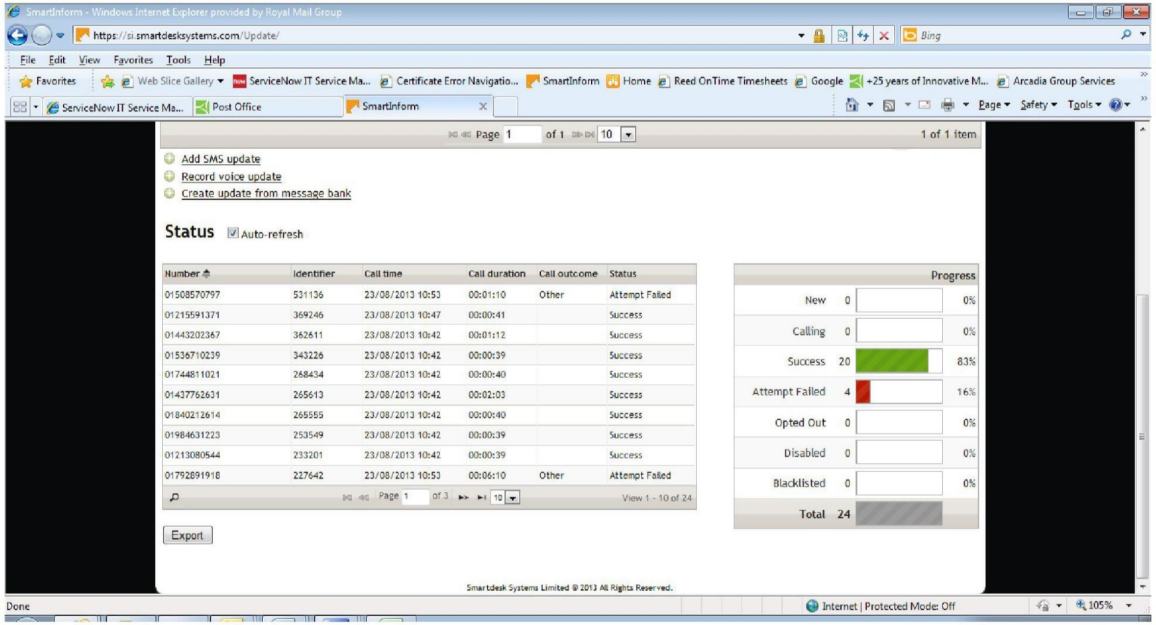
Pageone is used to send out text messages and emails to set groups. We just page one to send out comms to the wider business usually for incidents that are business impacting.



POL00398160

11.4. Smart Inform – Direct dial message to branches

This is a application that allows Post Office to send prerecord voice meassgaes to branch telephones. It is another tool that is very useful in getting information to branches.



POL00398160

11.5. MemoView – Message to Branch Horizon System

A memoview is used to send short message to branches. It will go to all the horizon terminals and can remain on the screen for serveral weeks if needs be.

Sent to all branches

MBS 213 - Horizon report

The Post Office has today announced the introduction of an independent mediation scheme to address the concerns raised by some subpostmasters regarding cases which they feel require further resolution.

This follows the publication of the interim report into the Horizon system produced by Second Sight in July.

The report stated that so far no evidence of system wide problems with the Horizon software had been found. However, it noted that improvements could be made in the training and support processes provided to subpostmasters.

In response to the report the Post Office has made a number of commitments, one of which is to create this independent mediation scheme for subpostmasters and the Post Office to investigate and try to resolve subpostmasters concerns.

The Post Office statement will be available on Subspaceonline and [HYPERLINK "http://www.postoffice.co.uk/news-releases-2013"] this morning.

POL00398160

11.6. Twitter – Direct Communication with Customers

POL00398160

13.Appendix F – Manual Incident Logging form

POINT OF CONTACT

Once completed, this form must be sent to the Information Security Manager via email

Name	*(Name).*	**Telephone**	*(Telephone)*
Email	*(email)*	**Department**	*(Department)*

NATURE OF INCIDENT

	Service Failure	*No*	**Lost/Stolen USB device**	*No*
	Information Breach	*No*	**Virus/Trojan/ Worm**	*No*
	Network Issue	*No*	**Fraud/Scam**	*No*
	Data Centre Issue	*No*	**Website defacement**	*No*
	Denial of Service	*No*	**Distributed DOS**	*No*
	Intrusion / Hacker	*No*	**Probe / Scan**	*No*
	Customer Escalation	*No*	**System misuse**	
	Other	*(please specify)*		

Note: in case of stolen laptops/ IT equipment, particularly if stolen away from the office, i.e. from home, the incident must be reported to the police and a crime number obtained.

INCIDENT DETAILS

Provide details of the incident that you are reporting, include the date and time (if possible) and the names of any individuals involved.

Description	*(please specify)*			
Cause of Incident (who, what, where, when how)	*(please specify)*			
Damage Assessment (systems, services, etc.)	*(please specify)*			
Incident Timing	**Start/Occurrence**	*(Start)*	**End**	*(End)*

POL00398160

Information Compromised?	Has sensitive information relating to business activities, customers or staff been, or suspsected as having been compromised?	
	No	
	Specific details to describe the information (data) 'At Risk'	*If yes please provide details of the nature of the information, i.e. cardholder data personal details such as names, addresses, or business sensitive data (e.g. financial, commercially sensitive) has been compromised*

NOTIFICATION PROCESS

Include every step in the notification process	*(please specify)*
Automated monitoring notification	*(please specify)*
An infrastructure team member noticed something out of the ordinary	*(please specify)*
A user called in	*(please specify)*
Detail the flow of the incident response	*(please specify)*
Communication of resolution of the outage	*(please specify)*

FIX ACTIONS

Summary	Summary of actions undertaken to fix the incident	
	(Specify including details of troubleshooting, changes (configuration, hardware, etc), steps to confirm the outage was resolved)	

CONCLUSIONS

Summary	Summary of actions undertaken to fix the incident

POL00398160

What was basic cause of incident?	*(please specify)*
What would have prevented this?	*(please specify)*
What was the impact?	*(please specify)*
What was business criticallity?	*(please specify)*
What are the estimated impact costs?	*(please specify)*
What prevents incident from reoccuring?	*(please specify)*
What additional actions need to happen?	*(please specify)*

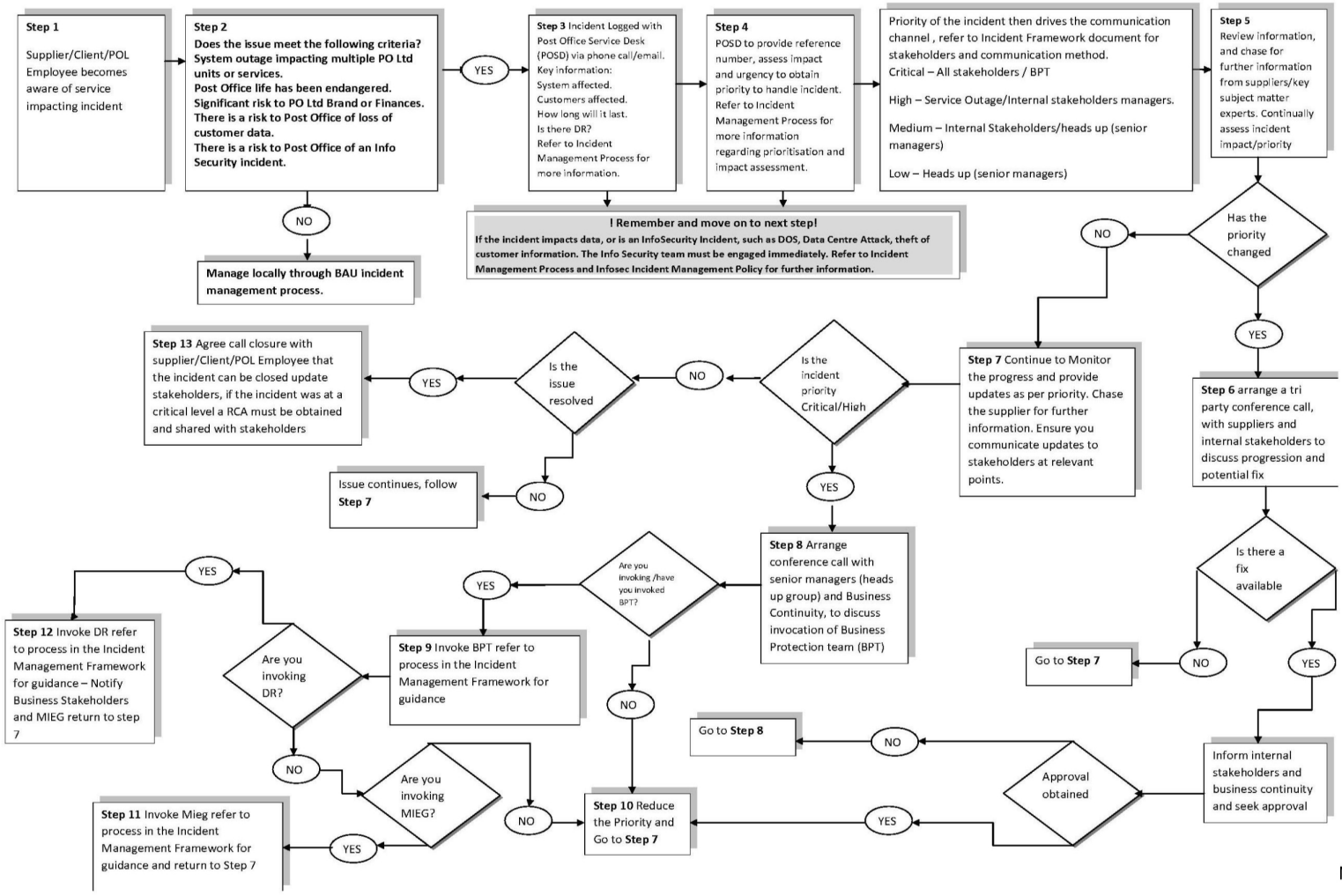
APPENDIX

Files	*(List of files/documents that underpin this Report)*

POL00398160

14.Appendix G Incident Management Process

Incident Management Process is detailed below. The attachment also contains the step through diagram and process flow.



POL00398160

15.Appendix H – Post Incident Analysis Template

INCIDENT DETAILS	
Customer	
Service Affected	
Incident Reference numbers	
Date and time of Incident	
Total Outage Time	

Customer Impact and Description of Incident

Root Cause/Fix

Customer Highlighted Issues

Observations and Corrective Actions

Action Plan to be owned/progressed by Service Delivery Manager

Action	Owner	Status	Date of Completion

Timeline – Key Events

-
- .
-