Granby Marketing Services Business Continuity Plan
Plan 2

May 2015

Site Unavailable

Contents

Section 1: Company Objective For BCP

The objective of this Business Continuity Plan is to create a document that will list actions, contacts and responsibilities that will lead to the recovery of all or any business functions that may be affected by a disaster or crisis within a time frame that allows for the shortest practicable time of disruption.

This plan is one of a group of plans that together, with approval from senior management, consist of the overall organisational Business Continuity Policy and Strategy.

Additionally the company BCPs work towards compliance with BS259991:2006 and the Business Continuity Institute Good Practice Guidelines.

Section 2: Business Continuity Team

The Business Continuity Team consists of the following personnel:

Joanne Varey – Managing Director – 07989 353462
Janet Carter – Financial Director & HR – 01254 604689
Andrew Gregson– Head of Client Delivery – 07977 018381
Marc Dobney – Planning & Implementation – 01254 503599
Dave Saunders – Head of Operations – 07989 353437
Matt Lancashire – Head of IT - 07823338280

The above mentioned names will be the first point of contact in the event of crisis or disaster involving their owned departments.
In the event of the named departmental manager not being available the following personnel will deputise:

Joanne Varey for Finance - 07989 353462
Dave Saunders for Planning and Implementation – 07989 353437
Jen Ross for Human Resources Management – 01254 604689
Andrew Gregson for Operations Management – 07977 018381
Leon Robinson for IT – 01254 604117

Section 3 – Plan Scenario

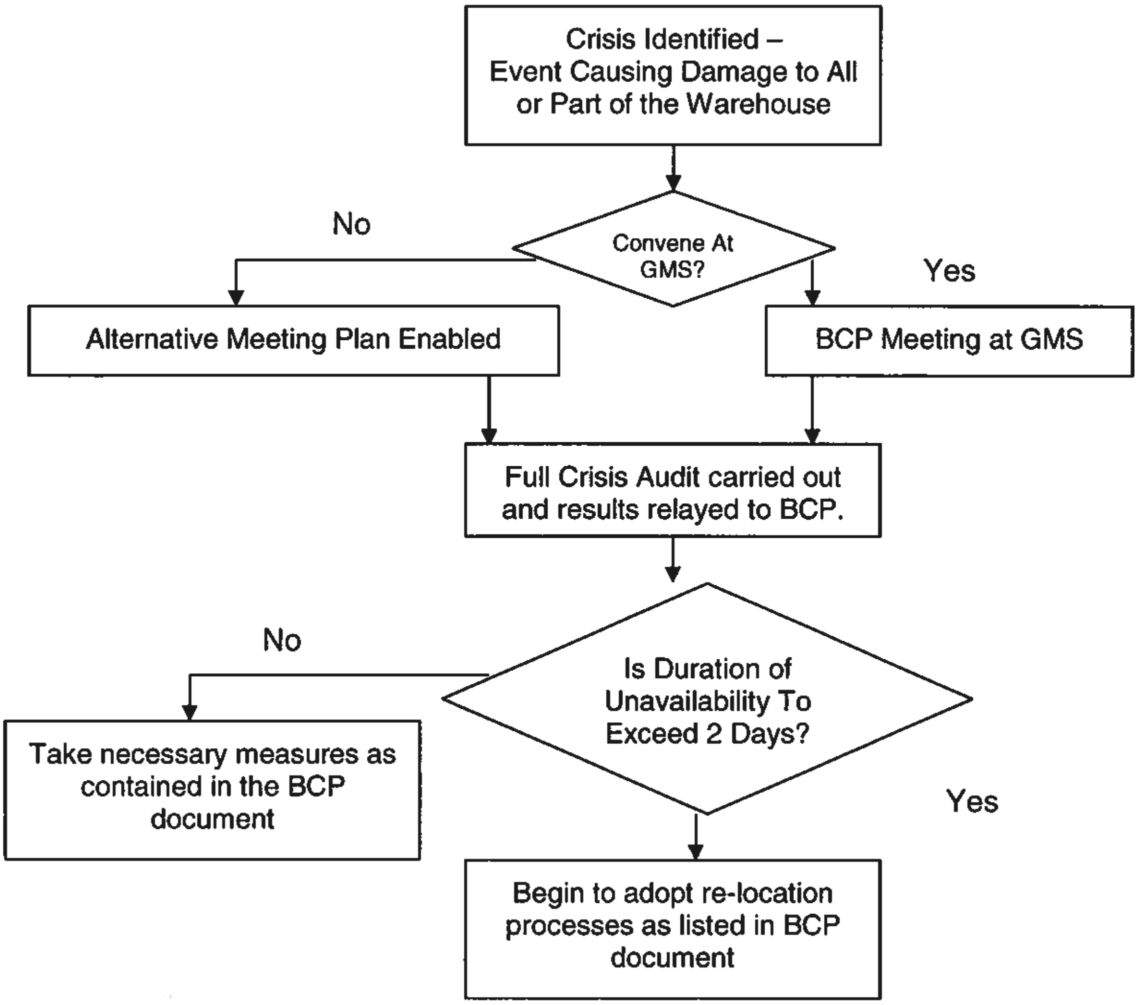
The Site Unavailable plan has been formulated to provide a list of responses to ensure business continues for Granby Marketing Services in the event of this occurring.

Section 4 – Business Impact Analysis

Operational impacts are rated on a scale of 0-4 where 0 = no impact and 4 = sever impact. The impact value is an indication of the severity of the impact to the company that would result if the planned scenario occurred.

Operational Impact	Value
Service to Client	4
Service from Suppliers	4
Staff Morale	2
Cash Flow	3
Regulatory	1
Physical Infrastructure	1
Systems Infrastructure	1

Section 5 –Workflow


Crisis Identified – Event Causing Damage to All or Part of the Warehouse
Convene At GMS?
No
Yes
Alternative Meeting Plan Enabled
BCP Meeting at GMS
Full Crisis Audit carried out and results relayed to BCP.
Is Duration of Unavailability To Exceed 2 Days?
No
Yes
Take necessary measures as contained in the BCP document
Begin to adopt re-location processes as listed in BCP document

SITE UNAVAILABILITY

#	Description	Owner	Time Scale
1	Undertake full impact on building & stock & risk assessment & contact Insurer via Finance	Ops Manager	Day 1
2	Undertake full impact on IT Systems considering operator access in view of the ops manager assessment. If required commence re-location plans. If unavailability < 2 days begin remote control of all systems in line with plan.	IT Manager	Day 1
3	Begin locating temp workspace for account managers and retrieving documents. Begin consulting with clients re: effects and likely durations.	Head of Client Delivery	Day 1
4	Inform all staff of incident, likely duration & likely outcome.	Financial Controller	Day 1
5	Begin re-location of any stock & other resource that remains accessible to alternative locations in line with plan & expected duration of incident.	Ops Manager	Day 1
6	Ascertain whether relocation plan is to be implemented - if it is contact landlords & couriers	Financial Controller	Day 1
7	Ensure affected area has adequate security	Financial Controller	Day 1
8	All ops depts to ascertain impact on immediate staff and work loads in line with #1 - schedule staff, resouce & activity accordingly	Ops Manager	Day 1 -2
9	Inform PR of issues and anticipated duration	Head of Client Delivery	Day1 - 2
10	IT to instigate back up server plan in conjunction with BCP IT Partner & begin process of implementing operational processes if incident goes beyond 2 days.	IT Manager	Day 2
11	Acquire access to alternative IT resource and ensure clients are contactable via usual methods.	Head of Client Delivery	Day 2
12	Ensure new location utilities are available and meters read if relocation takes place.	Financial Controller	Day 2
13	Relocate affected departments in line with resource and stock.	Ops Manager	Day 2

14	Ensure resource is available for Communications Centre relocation in line with BCP Partner and in line with BCP Plan	IT Manager	Day 2
15	Ensure resource is available for staff to relocate to supplied alternative resource	Financial Controller	Day 2
16	Ensure resource is available for removal of stock to new facility and that all stock transferred is recorded along with any other manual activity.	Ops Manager	Day 2
17	Continue adopting re-location plan if required	Ops Manager	Day 2 - Ongoing
18	Ensure staff are suitably located & informed of all current and short term issues	Financial Controller	Day 2 - Ongoing
19	Ensure all systems, including comms are adequate and business can continue to function over the required sites.	IT Manager	Day 2 - Ongoing
20	Ensure records of all associated costs of incident are logged and recorded	Financial Controller	1 Week
21	Quantify client insurance claims if appropriate	Head of Client Delivery	1 Week
22	Ensure all ops depts are working efficiently	Ops Manager	1 week onwards
23	Ensure HR are communicating all developments to all staff	Financial Controller	1 week onwards
24	If unavailability continues over 10 days maintain and review all systems to ensure that all resource is adequate and robust and that all departments are functional.	IT Manager	1 week onwards

Section 7 – Communications Plan

The external communications to non clients (i.e. industry media) will be managed by the company appointed PR Agency - **LIMELIGHT**.

Contact Details:- 20
Grosvenor Place
London
SW1X 7HN
Tel: 0207 201 0600
Fax: 0207 201 0601

Section 8 – Claims Procedure

ALL STAKEHOLDERS IN THIS PLAN MUST BE AWARE THAT ONLY IN

CIRCUMSTANCES WHERE HEALTH AND SAFETY OF INDIVIDUALS IS IN JEOPARDY MUST ANYTHING BE MOVED BEFORE THE LOSS ADJUSTORS HAVE BEEN TO VISIT THE AFFECTED SITE.

Claims and Initial Contacts must be directed to:

Watson Laurie Ltd
Watson Laurie House
234-236 St Georges Road
Bolton
BL1 2PH

Tel:- 01204 387111

Section 9 – Call Centre Re-Location Plan

Granby Marketing Services Business Continuity Plan

Communications Centre Re-Location Plan

Plan to be followed in the event of Communications Centre Requiring Re-Location

Communications Centre Manager to be the Owner of All Actions though these may be delegated as appropopriate.

1/ Ascertain size of area required and locate an appropriately sized location (bearing in mind also Storage requirements, if any) from one of the contacts listed below.

The location would need to fulfil the following criteria:

- Easy Egress
- Secure
- Capable of hosting networked PCs via remote links • Capable of hosting multiple simultaneous telephones

Easy Offices – 0870 240 8378 – www.easyoffices.com - info@easyoffices.com

Makeitlancashire.com -
http://www.makeitlancashire.com/?q=propertysearch
Username – Mdobney@granbymarketing.com
Password – SAKGMS

Trevor Dawson Estate Agents - 01254 681133 -
http://www.tdawson.co.uk/property-register.asp

2/ IT to move into site and audit site for:

- Suitability of Power and Network Capabilities
- Capability of Remote Network Access
- Capability of Simultaneous Telephone Hosting

3/ If site appropriate IT to obtain PCs and Telephones either recovered from GMS or rented from:

Blaze Computer Rentals – 0844 800 3324 info@blazecomputers.co.uk
http://www.blaze-computers.co.uk/laptop-hire-manchester.html

Computer Hire UK – 0118 986 1133 sales@rentaloptions.co.uk
http://www.rentaloptions.co.uk/

Hamilton Rentals – 01344 456600 info@hamilton.co.uk
http://www.hamilton.co.uk/overview.cfm

and wire up and fit PCs to plugs and networks, ensuring IT operator checks the connection to the BCP Servers are connectable and working.

4/ If site appropriate IT to contact NGC and arrange the installation of recovery telephony system for amount of seats as determined and requested by Call Centre manager.

NGC Networks – 0800 588 4003 info@ngcnetworks.co.uk
http://www.ngcnetworks.co.uk/

IT to liase with NGC to ensure all DDIs and client numbers for operational work are set up correctly and available for use.

5/ IT operator to implement the Remote Scope Access logins across all the PCs that have been set up and supply written instructions to the Communications Centre manager.

6/ Communications Centre to move into new area and supervisor to take responsibility for ensuring the premises conform with appropriate H&S legislation including heat, light and security and escalate any issues to their immediate line manager.

7/ Supervisor to contact all staff and make sure they are able to commute to the new location and are available for working in liasion with HR contact plans.

8/ Scope administrator in liasion with DP supervisor to contact all interested parties, including the Royal Mail, DHL and all suppliers of mail, and make them aware of the new premises the mail needs to be delivered to.

Section 10 – Alternative Meeting Place Details

1) – Blackburn Enterprise Centre 01254 505 000
lorraine.bradley@blackburn.gov.uk

2) – Eanham Wharf – Blackburn
01254 503500

Royal Mail Group's Approach to Business Continuity

Introduction

Royal Mail recognises the critical importance that our services provide to our customers and in turn to your customers.

For this reason we have adopted a managed programme approach to Business Continuity (BC), which is aligned to the British Standard for Business Continuity BS25999. The new International Standard ISO 22301 is currently being evaluated. The programme is endorsed at Board level with the Managing Director of Royal Mail Operations and Modernisation having overall responsibility for deployment.

Our Business Continuity programme has been independently audited by the Head of Business Continuity at a leading firm of consultants, who concluded that Royal Mail Group is already 'Broadly compliant with the demands of BS25999' The programme is overseen by a group of BC experts from within the business, who strive for continual improvement.

Royal Mail Group is a Gold sponsor of the BCI. For confidentiality reasons Royal Mail Group does not share details of our BC Management Programme with customers but we are happy to talk through our approach.

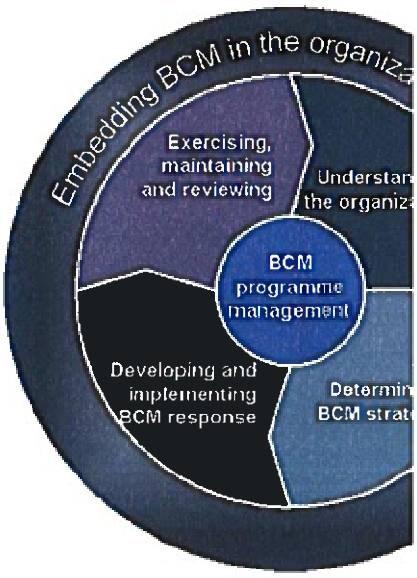
Our approach to testing is one of continuous improvement. We believe there is no better test of continuity plans than responding to real live incidents. Given the size of Royal Mail Group (we have over 1,400 sites) we are responding to incidents on a regular basis e.g. severe weather over the winter, suspect items, fires, floods and riots. At the end of each incident we review all of our planning and lessons learnt trigger an update of our materials.

All significant incidents our handled by our 24/7/365 Central Postal Control (CPC) who log and assess each incident and deal with or escalate as necessary. CPC provide details of all incidents internally which our Customer Services and Account Teams draw off to continually update their clients as appropriate.

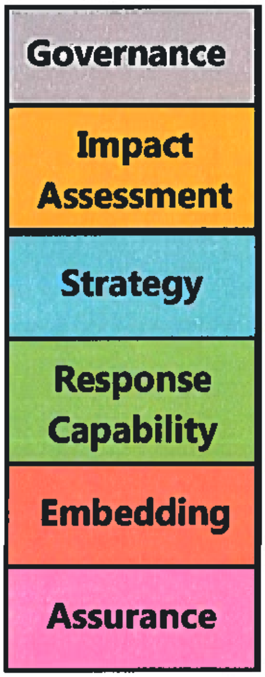
A Programme Approach

Our programme is led by a dedicated fulltime Business Continuity Team. Below is an illustration of how our programme is aligned to the lifecycle approach promoted in BS25999

The Business Continuity Lifecycle represents the Programme continuous operation of the business within Royal Mail Group


Embedding BCM in the organiza
Exercising, maintaining and reviewing
Understan the organiz
BCM programme management
Developing and implementing BCM response
Determin BCM strat

Royal Mail Group BCM Continuity programme


Governance

Impact Assessment

Strategy

Response Capability

Embedding

Assurance

An explanation of each element of our programme is contained within this briefing

Governance

Scope

The Royal Mail Group BCM policy and supporting BCM minimum standards apply to all business units and Group support functions. Responsibilities are divided under three headings:

- **Planning** – developing business continuity and incident management plans;
- **Response** – dealing with actual incidents and disruptions;
- **Assurance** – ensuring appropriate plans and arrangements have been made.

Planning

The key responsibilities for planning are as follows:

The **Risk Management Committee (RMC)** operates at Royal Mail Group level

- Approval of the Royal Mail Group BCM policy
- Ensuring that resources are made available across the group as required
- Confirmation of the key risk scenarios to be used for planning purposes

Internal Audit & Risk Management (IA&RM) operates at Royal Mail Group level

- The development and maintenance of the Group BCM policy
- The definition of minimum standards for BCM across the Group
- Reporting BCM progress and any issues to the RMC

Managing Directors of Business Units & Support Function Heads are responsible for:

- Appointing an executive to act as the BCM Champion for the business unit or support function
- Deploying resources to ensure that the business unit or supporting function develops and maintains its BCM capability so that it complies with the Group BCM policy and minimum standards
- Ensuring that a Business Protection Team (BPT) is in place for their business unit or support function. For details see Response Capability

The BCM Champions are:

- Responsible for ensuring that BCM is implemented in accordance with the requirements of the BCM policy and minimum standards
- Responsible for the identification of the key risks within their business unit or support function
- Supported by a full time business continuity team led by a senior manger who is responsible for the day-to day running of the business continuity programme

Response

The underlying principles for responding to and managing an incident are that:

- Business units and support functions are responsible for managing disruptions, including major incidents and crises that affect their own organisation, and for recovering their business.
- Once a team at any level has been activated, the leader of that team will immediately inform the leader of the next higher level team, who will decide whether or not to invoke their team. This is known as 'Tackle & Notify'
- Only if an incident has an impact across multiple business units or support functions or which impacts on the reputation and well being of Royal Mail Group as a whole will the Group Executive Business protection Team be invoked

Group Executive Business Protection Team (GBPT)

This is the top level incident management response consisting of the Chief Executive, Company Secretary and the directors of Operations & Modernisation, Commercial Regulated, Commercial Non-Regulated, Human Resources and Communications. Other directors or function heads may be coopted onto the GBPT as appropriate.

The team will take responsibility for key decisions, external communication with stakeholders, and the allocation of strategic resources during the crisis, whilst lower level teams will focus on the operational incident management and recovery.

Business Unit Business Protection Team (BPT)

This is the senior team within each business unit or support function the core of which is the Managing Director (MD) or support function head, supported by the BCM Champion, and an extended pool of resources covering Communications, HR, Legal, Facilities, IT, Finance, Operations and Security.

The BPT provides the top level of incident and crisis management and support within the business unit or support function, and an appropriate and timely response consistent with the BCM policy.

This covers operational prioritisation and decision making, internal and external communications and the mobilisation of resources to manage the incident and to co-ordinate restoration and recovery.

Once a BPT is activated, the leader of the GBPT must be notified by the BPT leader.

Further details are shown under Response Capability

Assurance

The **Risk Management Committee (RMC)** provides top level oversight of BCM on behalf of the Group Executive Team (GET) and of the Audit & Risk Management Committee (ARC) of the Royal Mail Group Holdings Board and is accountable for:

- Sustaining the appropriate level of assurance for BCM activity; ➢ Reporting BCM status and issues to the ARC and the GET.

The **Internal Audit & Risk Management Committee (IA&RM)** acting on behalf of the RMC is accountable for:

- Ensuring that the BCM policy and minimum standards are reviewed annually and benchmarked against industry standards and best practice;
- Developing a self-assurance protocol for business unit and support function heads to use that will provide assurance and evidence that business units are complying with the minimum standards;
- Providing high level assurance that the BCM policy is being complied with;
- Business Unit Heads and Support Function Heads are accountable for deploying the resources to provide the assurance and evidence that the business unit or support function complies with this policy and the supporting minimum standards.

Impact Assessment

A Risk and Business Impact Assessment has been conducted to identify the Risks and Threats to our Network and identify the impact on our customers and Royal Mail Group's reputation should these occur.

The assessment has identified five broad categories which along with the main sub-categories are shown in the table below. These have informed our planning priorities.

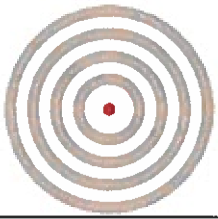
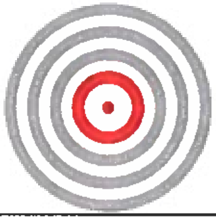
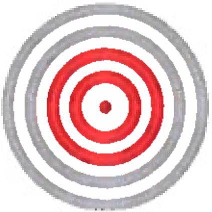
Main Category	Sub- Categories / Examples
Environmental	➢ Severe Weather - snow, ice, storm, flooding etc ➢ Fires
Major Health Alerts	➢ Potential Flu Pandemic ➢ SARS ➢ Foot & Mouth
Supplier Failure	➢ Fuel ➢ Technology ➢ Utilities - power outages
Industrial Action	➢ Local unofficial action ➢ Official action either local, regional or national
Terrorist Activity - CBRNE	➢ London 7/7 scenario ➢ Royal Mail Group used to deliver dangerous items e.g. Anthrax, Explosives

Strategy

Previously Royal Mail Group won the 'Crisis Strategy of the Year' (and was short listed for two other awards) at the annual BC industry awards.

At the heart of the strategy is a series of five integrated incident response manuals each addressing a specific audience and providing scalability in our response from an incident at one specific site to incidents with national geographic reach (e.g. severe weather, flu pandemics)

Once a team at any level has been activated, the leader of that team will immediately inform the leader of the next higher level team, who will decide whether or not to invoke their team. This is known as 'Tackle & Notify'

	**Be Aware** Suspect items remain Royal Mail Group's most frequent type of incident, with the potential of leading to serious business interruptions. The Be Aware booklet contains easy to follow advice and has been issued to all operational managers resulting in a 80% reduction of stoppages
	**Stay Calm** Each Person in Control (PiC) for every Royal Mail Group site has been issued with a Stay Calm manual which guides the user through key principles of handling a wide range of incidents helping to reduce the potential period of operational stoppage / business interruption at the affected site.
	**Be Prepared** Should an incident at a Royal Mail Group site lead to a wider business interruption, each of the 5 Geographic Leadership Teams have an incident response team which can form quickly, and aided by their Be Prepared manual can manage the situation and invoke the relevant continuity plans in accordance with the agreed business priorities.

	Take Control All incidents are reported to Central Postal Control who will assess the impact of the incident and if necessary invoke the Business Protection Team or if not necessary will monitor the situation until
	the incident can be closed
	Take Action The BPT will form for major incidents and will use Take Action as a prompt to consider all the key aspects of handling a response, especially developing a stakeholder communications plan.

Response Capability

Our response capability is built around our award winning 'Crisis Management Strategy' outlined above.

All incidents are reported to our 24x7x365 control centre who make an initial assessment as to its severity and potential impact. Thereafter they co-ordinate the deployment of any required contingencies whilst a team of senior managers drawn from all disciplines across the business (known as the Business Protection Team (BPT) work together to recover 'business as usual'

The precise make up of the BPT will vary dependant upon the nature and severity of the incident. E.g. Technology issues would be led by out IT specialists, flu pandemic preparedness by our medical doctors and health teams etc

Our capability is aligned to (but not constrained by) the Risks and Threats identified in our impact assessment. For example, some 'left of field' incidents such as the closure of UK airspace caused by the Icelandic volcano ash cloud were dealt with by deployment of our standard contingency plans for airport closure more usually triggered by severe weather / fog or individual aircraft failure.

Generic Capabilities

The sheer scale of the Royal Mail Group operation means that in addition to the specific capabilities outlined above we have a unique ability to flex our operation meaning that many incidents such as vehicle breakdowns, aircraft failures, road closures, increased volumes e.g. large mailings are managed as business as usual.

We work with our customers to identify and plan for all major mailings. We have a Key National Posting team who are able to co-ordinate activity to ensure a seamless service- an example of this is our work with both central and local Government during election periods and our work on the last National Census.

Our Network

Every day we collect from over 115,000 post boxes. On average we sort and deliver 62 million items of mail to 29 million addresses in the UK. In addition to this our ability to flex our entire operation is demonstrated every year at Christmas

Our People

We employ over 130,000 people and can access additional working hours either through overtime or where necessary using fully vetted temporary staff,

Our Premises

We have over 40 mail and distribution centres and over 1,300 delivery offices. All of our operational sites have their own plans, based on the central policy principles, which are reviewed regularly. During the last incident at which there was catastrophic building damage to one of our sites, (a fire at Northampton Mail Centre) our contingency arrangements allowed Royal Mail to establish a delivery operation from scratch, comprising 350 delivery routes serving around 150,000 addresses, in a little over 24 hours, enabling Royal Mail to resume deliveries in the NN1-7 postcode areas. Deliveries across the remaining NN postcode areas continued as normal throughout this period.

Our Vehicles

Our fleet consists of over 33,000 vehicles and can be flexed as required via contracts that enable us to hire additional vehicles at short notice.

Our vehicle fleet is maintained by our national vehicle workshop facilities, which provide 24 hour servicing and emergency breakdown cover. Reserve vehicles are held at all main sites and vehicle workshops.

In the event of vehicles breaking down or being involved in an emergency, drivers will contact their local hub as soon as it is safe to do so. If the vehicle can be repaired within one hour, the driver will continue deliveries. In the event of the vehicle being unserviceable, an alternative vehicle is provided and our Customer Service Centre advises the customer of any delays.

Other specific examples of our capability are shown below:

Severe Weather 2010-11

- Conference calls were held daily between our 24x7x365 control centre and the operational regions throughout the adverse weather to assess the latest weather conditions, receive updates from local units on how the operation was being affected and to amend contingency plans for the next few hours or overnight
- Arrangements were put in place to ensure that our corporate priorities were managed effectively and that the most time critical mail was managed to minimise the impact on service.
- Extra vehicles were requisitioned where available to deal with mail that was unable to be flown, either due to the entire airport being closed, or runways being closed to clear snow and ice build up, or where conditions were deemed too unsafe to operate.
- Mail Centres and Delivery Offices carried out daily risk assessments collecting and delivering mail where conditions would allow.
- Business and domestic customers were kept apprised of the unfolding situation and the effects on service
- A Daily Operations Statement was prepared to update Royal Mail customer facing staff on the current operating position, how deliveries were being affected, how distribution through the air network had fared overnight along with a prognosis on the likely areas worst affected by residual and fresh snowfalls. The daily operations customer statement was issued to around 5000 customers (primarily business customers)
- Weekly service update bulletins were also written for business customers, cascaded by business customer teams
- The Sales and Customer Services teams, who look after our largest account managed segments, had around 24,000 conversations to update customers about how the weather was affecting service during the first three weeks of January and how Royal Mail Group was responding.
- When the severe weather was over a 'Severe Weather Working Group' was established to review all the plans and materials deployed during this period and to share and evaluate local initiatives with a view to identifying and codifying best practice. Enhanced preparatory planning and assessment tools developed by this group have already been deployed ready for the next severe weather.

Influenza Pandemic

- Royal Mail Group's Head of Health is a medical doctor who enjoys excellent links to a variety of UK and worldwide health agencies and has led on providing medical advice to our plan which is entirely consistent with the advice being given by the UK Governments Health Protection Agency.

- Our plan has followed planning assumptions which are common to most other companies.
- We have benchmarked our plans against a wide range of other companies and with business continuity experts - to identify any gaps / further improvements.
- Royal Mail Group has conducted a planning exercise in conjunction the Cabinet Office to provide a pan-UK view.

Key Supplier Failure

Fuel

- We hold our own fuel stocks as this gives us the maximum economic and operationally efficient solution. Fuel for our fleet is purchased in bulk and bunkered at most operational sites thereby providing a contingency supply. For further contingency purposes, we have access to additional fuel reserves as well as alternative sources of storage e.g. rail tankers.

Technology

- A major incident response process and team are in place
- Risk & Business Impacts have been determined for critical systems
- We have a number of back up datacentres across Europe ➢ The majority of systems are tested annually

Terrorism - CBRNE (Chemical, Biological, Radiological, Nuclear, Explosives)

- A working group has been in existence since Autumn of 2001 as a consequence of the anthrax attack via the post in the US.
- Royal Mail Group has experienced thousands of suspect powder and bomb alerts which can be very disruptive to our operations. This led to the production of the award winning 'Be Aware' booklets containing simple advice and has been issued to all operational managers. This has helped improve our response to these incidents, greatly reducing service disruption.
- Over the years we have run four national and over 30 local desk top simulation exercises,- with relevant Emergency Service personnel in attendance have been conducted. to develop and refine our response.
- Royal Mail Group and the Department for Business, Innovation and Skills (formerly BERR & DTi) have held joint exercises enabling a wide cross

section of Government departments and agencies to explore how the Government and Royal Mail Group would respond to an anthrax attack.

- The provision of equipment to detect chemical, biological or radiological material passing through the postal system has been deployed to all our mail centres.

Embedding

The successful establishment of business continuity within a company is dependent upon its integration with both the strategic and day to day management processes and its alignment to business priorities.

Royal Mail Group strives to achieve this through an ongoing programme of

Training, Exercising, Awareness and Continual Improvement.

- Scenario exercises have been conducted with over 50 leadership teams
- 'Live' on site rehearsals are conducted with the Emergency services
- Bi-annual workshop with government departments
- Senior management reviews after major incidents e.g. severe weather during the winter of 2010/11 led to major enhancements to the preparation and assessment tools available to all levels of management
- Participation in the FSA Market Wide Exercise in 2009 and 2011
- Interactive business continuity workshops held at major mail centres
- Interactive Flu pandemic workshops held
- Coverage in 'Courier'. Employees magazine that goes to every employee

In addition our approach to testing is one of continuous improvement. We believe there is no better test of continuity plans than responding to real live incidents. Given the size of Royal Mail Group (we have over 1,400 sites) we are responding to incidents on a regular basis e.g. severe weather over the winter, suspect items, fires, floods, and riots. At the end of each incident we review all of our planning and lessons learnt trigger an update of our materials

Assurance

The **Risk Management Committee (RMC)** provides top level oversight of BCM on behalf of the Group Executive Team (GET) and of the Audit & Risk Management Committee (ARC) of the Royal Mail Group Holdings Board and is accountable for:

- Sustaining the appropriate level of assurance for BCM activity; ➢ Reporting BCM status and issues to the ARC and the GET.

The **Internal Audit & Risk Management Committee (IA&RM)** acting on behalf of the RMC is accountable for:

- Ensuring that the BCM policy and minimum standards are reviewed annually and benchmarked against industry standards and best practice;
- Developing a self-assurance protocol for business unit and support function heads to use that will provide assurance and provide evidence that business units are complying with the minimum standards;
- Providing high level assurance that the BCM policy is being complied with;
- Business Unit Heads and Support Function Heads are accountable for deploying the resources to provide the assurance and evidence that the business unit or support function complies with this policy and the supporting minimum standards.

It is also worth noting that:

- Royal Mail Group has been assessed by a leading consultancy as being broadly compliant with BS25999-2.
- Business Continuity is a condition of our licence to operate issued by our regulator Offcom and is assessed every two years.
- Royal Mail Group works closely with the Department for Business, Innovation and Skills (formerly BERR & DTi) on a range of business continuity issues. This provides an opportunity to benchmark our approach and share best practice across Government departments and agencies.
- Royal Mail Group is an active member and participant in industry best practice organisations such as 'AIRMIC' and 'London First'.

- Royal Mail Group is an active member of various European and National Postal special interest groups - dealing with security, health, and crisis management issues.

- On site compliance audits are conducted by independent verification teams.

SQA Business Continuity Policy 2015 v2.2

Policy and Programme Management

Background

SQA's Business Continuity Management System provides us with a framework that builds resilience through identifying and mitigating threats which have the potential to disrupt our business, whilst increasing our capability and effectiveness to respond to an incident. It ties in closely to SQA's wider risk management framework, to anticipate internal and external planned or unexpected events that have potential to disrupt SQA's business.

Purpose

The purpose of this Policy is to have a Business Continuity Management System (BCMS) in place that will allow SQA to provide:

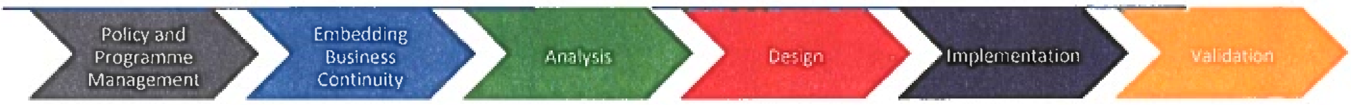
- plans to respond to an emerging incident
- immediate response to an unplanned and unwarranted event which would affect SQA's ability to function normally.

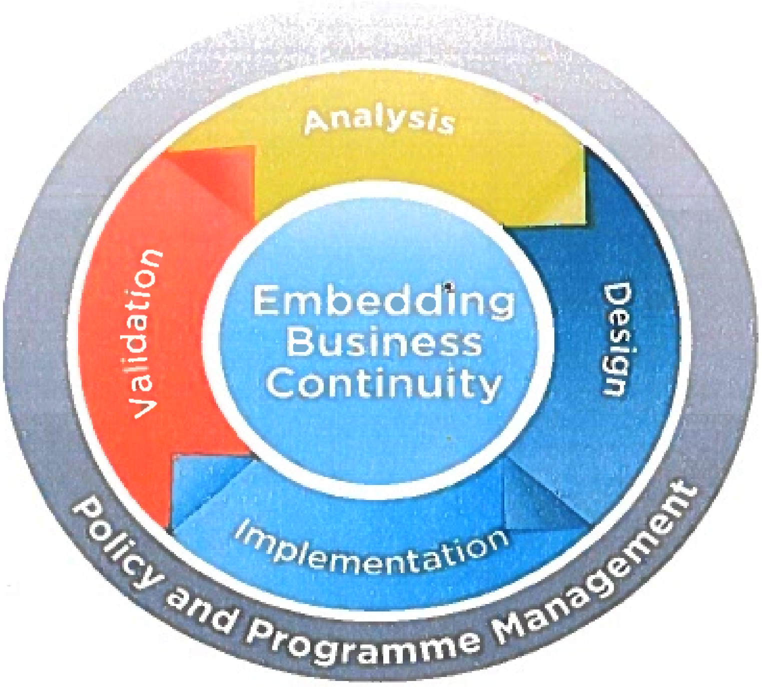
SQA's approach to BC management is based on the ISO 22301:2012 and ISO 22313: 2012 standards and the Business Continuity Institute Good Practice Guidelines GPG 2013.

Scope

This policy covers all of SQA, and all stages of the Business Continuity Management's lifecycle. It provides assurance to our stakeholders that we have plans in place to assist us in being ~~be~~-able to continue to provide critical services in the event of an incident, and it helps us safeguard our reputation.

The BCM Lifecycle is split in to Policy and Programme Management, Embedding, Analysis, Design, Implementation and Validation stages:


Policy and Programme Management
Embedding Business Continuity
Analysis
Design
Implementation
Validation


Analysis
Design
Implementation
Validation
Embedding Business Continuity
Policy and Programme Management

Source:

BCI Good Practice Guidelines 2013

Policy Statement

SQA is committed to:

- the enhanced safety of staff and appointees and its duty of care
- achieving Corporate Governance requirements, the prevention or mitigation and the control of the impacts of major incidents or emergencies
- embedding trust in the organisational culture
- protecting the organisation's reputation by a prompt, considered and professional response
- assuring potential commercial clients that contingency measures are in place
- providing external auditors with evidence to confirm that an effective BCMS has been implemented
- reducing the risk of litigation and corporate liability.

To support these commitments SQA will ensure that:

- a Business Continuity Management (BCM) System is in place
- Heads of Service recognise their responsibility for confirming their business continuity plans are accurate and current, and staff are aware of their plans and their individual responsibility
- business critical activities are identified and prioritised in the event of an incident

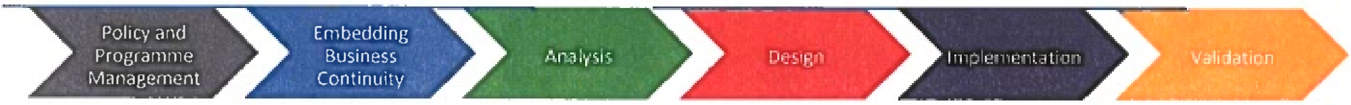
- the BCM team will manage the BCMS
- the BCM team will set up a schedule to review/monitor currency of plans
- the BCM team will facilitate the testing of the continuity plans and processes to ensure they are resilient and effective
- the BCM team will collate and maintain records on incidents that occur
- Strategic team and IMT to be aware of each team's respective roles and responsibilities and raise awareness to all staff
- the BCPs take cognisance of both external and internal changes that may impact on SQA's corporate or operational objectives
- effective internal communication processes are in place and tested and delivered through different mediums
- effective external communication to all stakeholders is in place and tested
- SQA liaises with key stakeholders in Scotland and at national level to ensure consistency of approach across the UK in dealing with a national incident.

Managing SQA's Business Continuity programme

In SQA, the Business Continuity Management Programme is an ongoing management and governance process led by the Director of Corporate Services who sponsors the BC Steering Group. This Steering Group includes representation from across SQA Directorates, and is supported by a Business Continuity Support Team which is part of SQA's Strategic Planning Team. Roles and responsibilities are outlined in Appendix A.

Embedding BCM in the Organisation's Culture

An ongoing training and awareness programme is in place to raise staff understanding of business continuity and how it is applied in SQA. The programme continues to heighten awareness through staff participation in refresher training, scenario exercises and articles in Inform.


Policy and Programme Management
Embedding Business Continuity
Analysis
Design
Implementation
Validation

Understanding the Organisation: Analysis of Business Impact and Continuity Requirements

SQA monitors risks to business continuity as part of their wider risk management framework. Risk registers and escalation procedures are in place for SQA Directorates and the transformational change programme. Registers are regularly reviewed to confirm that relevant risks have been identified and that appropriate mitigating actions have been agreed. Risks are escalated for management at the appropriate level up to the Board of Management.

The Business Impact Analysis (BIA) underpins SQA's BCMS, providing an understanding of the organisation's key objectives and how they are delivered. Updated annually, SQA's BIA identifies critical activities and the qualitative and quantitative impact of a disruption over time. It identifies related continuity requirements covering facilities, systems and data, and critical suppliers.

Design

SQA operates in a complex environment affecting, and potentially being affected by factors with the potential to disrupt, a diverse range of closely related and interdependent stakeholders. This is most acute in the delivery of National Qualifications through schools and colleges in Scotland. SQA is a key partner in the Scottish Government's Contingency Plan for the Qualifications System in Scotland. This Plan sets out a decision framework that brings together relevant partners to agree the best approach to minimise impact on candidates for any scenario which has potential to cause significant disruption to the qualifications system.

Designing SQA's BCM strategy

SQA has defined continuity strategies for facilities, systems/ data and suppliers. These are updated to reflect changes in business requirements identified through regular refresh of the Business Impact Analysis.

The purpose of the business continuity strategy is to ensure that SQA has processes in place to identify potential risks that could cause severe disruptions and the ability to respond immediately to an incident that would have a major impact on the delivery of SQA's critical activities. The strategy is based on a mixture of:

A pro-active approach:

□ Identifying potential risks to SQA from the internal and external environment.
□ Risk mitigation (prevention and protection measures).

A re-active approach:

- Identification of critical activities and resources depending on time of year and business priorities.
- Recovery of prioritised IT services within 48hrs – 72hrs.
- Procurement of other replacement IT equipment 'at time of disaster'.
- Securing alternative accommodation and facilities to support critical activities.
- Reputation management and communications. □ Relocation of affected staff to:
  - available SQA office accommodation in any unaffected units (e.g. "spare" space such as training rooms and meeting rooms, and by displacing "non-essential" staff).
  - other SQA locations.
  - where applicable, to work from home or other suitable locations (e.g. customer/supplier sites, local hotels, etc).

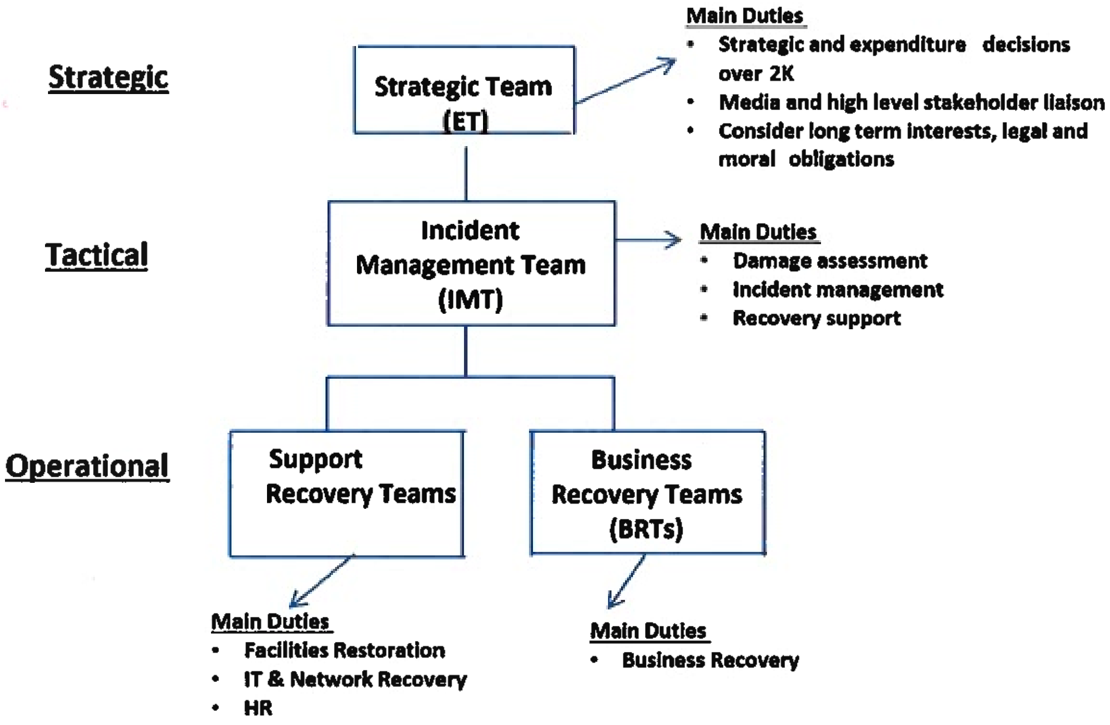
Incident response Structure

SQA incident management structure is formed by 3 levels, the Strategic Team (EMT), the Incident management team (IMT) and the Business Recovery Teams (BRTs). In an incident, SQA operates a command and control structure. This command and control structure supports an organised response to an incident and provides the ability to apply effective recovery processes. This approach also defines roles and responsibilities at strategic and tactical levels as well as supporting the internal and external communications strategy.

The diagram below illustrates the structure for incident response and recovery within SQA.

Incident Management Team Information

In an incident, SQA operates the command and control structure below:



Strategic

Strategic Team (ET)

Main Duties
- Strategic and expenditure decisions over 2K
- Media and high level stakeholder liaison
- Consider long term interests, legal and moral obligations

Tactical

Incident Management Team (IMT)

Main Duties
- Damage assessment
- Incident management
- Recovery support

Operational

Support Recovery Teams

Main Duties
- Facilities Restoration
- IT & Network Recovery
- HR

Business Recovery Teams (BRTs)

Main Duties
- Business Recovery

Any staff identifying a potential disruptive event should raise their concerns with their Head of Service or any other senior manager available. The Head of Service will evaluate the impact with the aid of the incident grid below and decide whether to invoke the incident response arrangements. SQA has identified three potential levels of disruption from minor to major incidents.

Invocation Grid

Incident	Characterised by	Response/ responsibility	Document/Plan

Green (minor incident)	• Localised disruption related to building or systems access • Widespread disruption <half day • Financial loss <£10k • Staff resources reduced by <10%	Local management responsible for resolution Informs IMT Coordinator to consider recommending invocation to Strategic Team Leader dependent on impact	**Business Continuity Policy.**
Amber (significant incident)	• Building or widespread systems access disrupted 1-3 days • Significant external threat identified (eg fuel crisis, industrial action) • Adverse media/ stakeholder interest	Relevant management (eg identifying manager or impacted manager) informs IMT Co-ordinator who agrees invocation of IMT Plan with Strategic Team Leader Strategic Team Leader places all members on standby	**Incident Management Team plan.**
Red (major incident)	• Damage or denial of access to building or systems for >3 days • Potential or actual risk to staff health and safety • Financial loss >£100k • Staff resources reduced by >40% • Significant adverse media/ stakeholder interest.	Relevant management informs IMT Coordinator who agrees invocation of IMT Plan with Strategic Team Leader. Strategic Team Leader invokes Strategic Team Plan	**Strategic Team plan.**
	□ There is a risk to the delivery of NQ qualifications and SQA's contingencies involve significant change to current delivery.	SQA Contingency Group, Qualifications Contingency Group	**Contingency Plan for the Qualifications System in Scotland.**

Developing and Implementing a BCM Response: Business Continuity Plans

SQA has plans in place to manage an incident, support recovery and to work towards resumption of business as usual. These plans are generic in order to respond to the impact

of a range of possible disruptions, rather than addressing specific scenarios. There are plans for Strategic, Incident Management and Infrastructure Recovery Teams. Due to the diversity of the organisation and the cyclical nature of its activities, each of SQA's business areas has its own BC plan. All plans are updated regularly and particularly whenever significant changes occur throughout the year.

Validation

Validation is the practice that ensures the BCM programme meets the objectives set in this policy and that the organisation's BCP is fit for purpose. Validation is achieved by exercising, maintenance and review.

Exercising

An exercise plan is in place to verify that, business continuity, business recovery and disaster recovery, plans, skills and resources are up to date and working effectively.

SQA carries out regular planned exercises and tests. These include tests of equipment and processes, individual team scenarios, and consolidated scenarios involving a number of areas of SQA. These normally include IMT, Facilities, IT, HR, Communications and required business areas.

Maintenance

SQA BC arrangements are kept up to date to ensure that the organisation remains ready to respond and manage incidents despite constant change.

The BCM team manages the maintenance schedule to ensure documentation is kept up to date and that is distributed to the relevant parties.

Heads of Service have the responsibility to ensure that plans are updated regularly and particularly whenever significant changes occur throughout the year. Changes can arise

Policy and Programme Management
Embedding Business Continuity
Analysis
Design
Implementation
Validation

from internal changes in structure and function, the external environment in which SQA operates, lessons learned in incidents and exercises, and identified improvements following a review.

Review

Following each exercise or live incident, a review is carried out to identify any improvements to SQA's Business Continuity Management System (BCMS).

SQA carries out an annual self-assessment process. The BCMS is reviewed by the BCM team and recommendations are presented to the steering group for approval.

BCMS is part of the improvement review plan carried out by our appointed internal auditors. Currently it gets reviewed every 3 years. The Audit Committee considers process improvement reports and monitors completion of agreed management actions.

Appendix A: Business Continuity Support Structure

Description	Responsibilities	Membership	Meeting schedule
BCM Sponsor	Sponsor the BC Steering Group Provide visible support of SQA's commitment to BCM at an executive level Liaise with and advise Scottish Government/stakeholders as appropriate	Director of Corporate Services	Ongoing
BCM Steering Group	**Objective** The purpose of the Business Continuity steering group is to provide strategic leadership and effective oversight of Business Continuity within SQA. The steering group will: • Ensure that adequate governance structures and control measures are in place • Ensure that relevant and effective policies are in place • Embed Business Continuity into SQA's culture • Ensure compliance with all relevant statutory obligations • Manage and provide oversight of ISO 22301, and alignment as required • Ensure that incidents are effectively managed • Ensure that SQA's suppliers are managed and audited effectively • Ensure that Business Continuity Management is adequately resourced	Director of Corporate Services (Sponsor) Haead of Strategic Planning and Governance (Chair) Business Continuity Management Team *Representation from all Directorates*	Four times per year
BCM Support Team (Strategic Planning Team)	Ensure that the organisation's business continuity plans, and related documents, are regularly reviewed and updated Promote business continuity across the organisation; administering the exercise programme. Keep the BCM programme updated through lessons learned and good practice.	Business Continuity Management Team	Ongoing

Heads of Service	Ensure that they maintain accurate and current business continuity plans for their own business areas. Raise awareness of BC within their teams.	All Heads of Service	Ongoing
SQA staff	Ensure awareness of BC within SQA Gain knowledge of their business area plan.	All Staff	Ongoing

Appendix B: Business Continuity Glossary

Business Continuity (BC)
The capability of the organisation to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Business Continuity Management (BCM)
A holistic management process that identifies potential threats to an organisation and the impacts to business operations. Those threats, if realized, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.

Business Continuity Management System (BCMS):
Part of the overall management system that establishes, implements, operates, monitors, reviews, maintains and improves business continuity.

Critical Business Function (CBF)
Vital functions without which an organisation will either not survive or will lose the capability to effectively achieve its critical objectives.

Contingency Plan
A plan to deal with specific set of adverse circumstances.

Disaster Recovery (DR)
The strategies and plans for recovering and restoring the organisations technological infra-structure and capabilities after a serious interruption. DR is now normally only used in reference to an organisation's IT and telecommunications recovery.

Exercise
Rehearse the roles of team members and staff, and test the recovery or continuity of an organisation's systems (e.g., technology, telephony, administration) to demonstrate business continuity competence and capability.

Incident

An event that has the capacity to lead to loss of or a disruption to an organisation's operations, services, or functions – which, if not managed, can escalate into an emergency, crisis, or disaster.

Incident Management Team (IMT)

A group of individuals responsible for developing and implementing a comprehensive plan for responding to a disruptive incident. The team consists of a core group of decision-makers trained in incident management and prepared to respond to any situation.

Resilience

The ability of an organisation to resist being affected by an incident.

Threat

A potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organisation, the environment, or the community. Some threats such as bad weather are more commonly referred to as “Hazards”.

Frontline
IT CONSULTANCY

Civica / MarkManager

Disaster Recovery / Service Failover Procedure

Public Use

Template History

Version & Date	Author	Revision Summary
1 17/12/2015	QH	First Draft
2 18/12/2016	TH	PMO review

Review

This document will be reviewed and updated as necessary:

- When required, to correct or enhance any content within the document.
- Following procedural or policy changes which Frontline adhere to.

Approvals

Name	Title
Lee Jones	Technical Services Manager

Distribution

Version & Date	Distribution
V1 18/12/2015	Published to Company via intranet for use/review
V2 22/07/2016	Published to Company via intranet for use/review
V3 04/08/2016	Changed document to Public Use from Internal Only & removed IP Addressing. LJ

Purpose / Scope

This document describes the process to successfully fail over the Civica / MarkManager iSeries based solution to the secondary hardware.

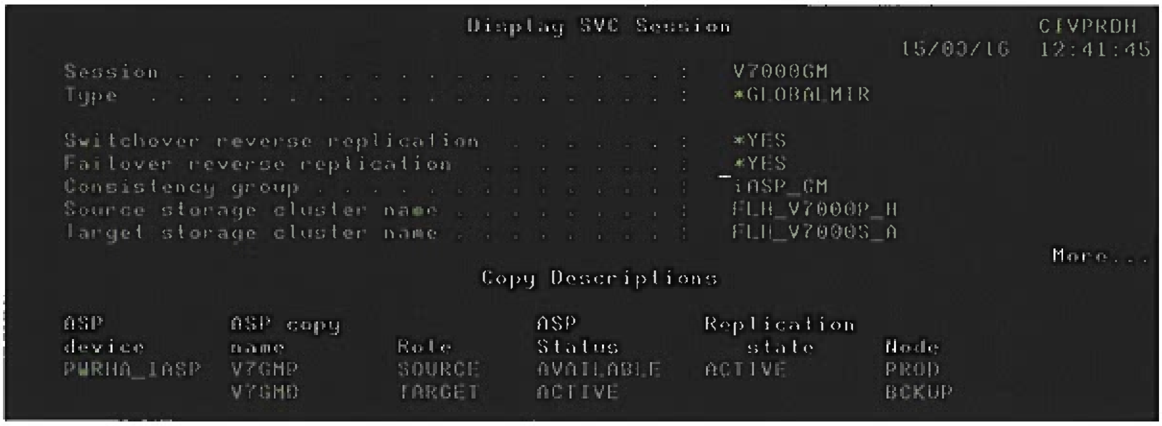
Contents

1. Planned Switchover

Note: It is critical the following commands are executed on the correct system.

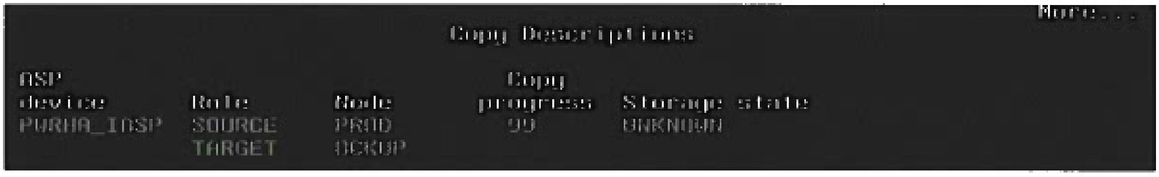
1/. On Prod machine -

DSPSVCSSN V7000GM - check working correctly. PROD node should have source role.



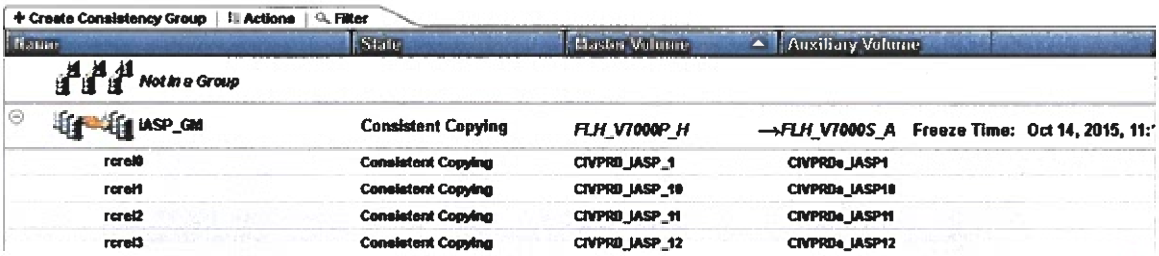
```
                           Display SVC Session                          CIVPRDH
                                                             15/03/16   12:41:45
  Session . . . . . . . . . . . . . . . . . . . :   V7000GM
  Type  . . . . . . . . . . . . . . . . . . . . :   *GLOBALMIR

  Switchover reverse replication . . . . . . . :   *YES
  Failover reverse replication . . . . . . . . :  _*YES
  Consistency group . . . . . . . . . . . . . . :  ‾iASP_GM
  Source storage cluster name . . . . . . . . . :   FLH_V7000P_H
  Target storage cluster name . . . . . . . . . :   FLH_V7000S_A
                                                                         More...
                           Copy Descriptions

  ASP          ASP copy                ASP          Replication
  device       name         Role       Status          state       Node
  PWRHA_IASP   V7GMP        SOURCE     AVAILABLE    ACTIVE         PROD
               V7GMD        TARGET     ACTIVE                      BCKUP
```

F11 *(note: Storage status unknown as this machine cannot sense remote status. 99% = max for Global Mirror)*



```
                                                                     More...
                        Copy Descriptions

ASP                                    Copy
device        Role        Node       progress    Storage state
PWRHA_IASP    SOURCE      PROD          99       UNKNOWN
              TARGET      BCKUP
```

Check FLNV7000_H *(xx.xx.xx.xx)* - check working correctly *(Note direction of arrow, to FLH_V7000_A)*



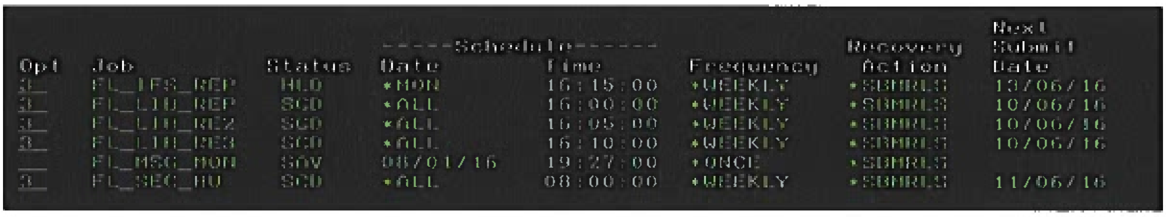
Name	State	Master Volume ▲	Auxiliary Volume	
Not in a Group				
⊖ iASP_GM	Consistent Copying	*FLH_V7000P_H*	→*FLH_V7000S_A*	Freeze Time: Oct 14, 2015, 11:'
rcrel0	Consistent Copying	CIVPRD_IASP_1	CIVPRDa_IASP1	
rcrel1	Consistent Copying	CIVPRD_IASP_10	CIVPRDa_IASP10	
rcrel2	Consistent Copying	CIVPRD_IASP_11	CIVPRDa_IASP11	
rcrel3	Consistent Copying	CIVPRD_IASP_12	CIVPRDa_IASP12	

Browse to "Copy Services," "Remote Copy" in the left hand pane.

2/. Before starting the Switch perform the following instructions on the PROD node:-

A). Sign-on as QSECOFR

B). Hold 4 x Job Schedule entries:-



```
                                                                            Next
                                 -----Schedule------            Recovery   Submit
Opt  Job           Status  Date       Time      Frequency       Action     Date
3_   FL_IFS_REP     HLD    *MON       16:15:00  *WEEKLY         *SBMRLS    13/06/16
3_   FL_LIB_REP     SCD    *ALL       16:00:00  *WEEKLY         *SBMRLS    10/06/16
3_   FL_LIB_RE2     SCD    *ALL       16:05:00  *WEEKLY         *SBMRLS    10/06/16
3_   FL_LIB_RE3     SCD    *ALL       16:10:00  *WEEKLY         *SBMRLS    10/06/16
__   FL_MSG_MON     SAV    08/01/16   19:27:00  *ONCE           *SBMRLS
3_   FL_SEC_BU      SCD    *ALL       08:00:00  *WEEKLY         *SBMRLS    11/06/16
```

C). End user jobs > CALL FL_PROD/FL_ENDJOB

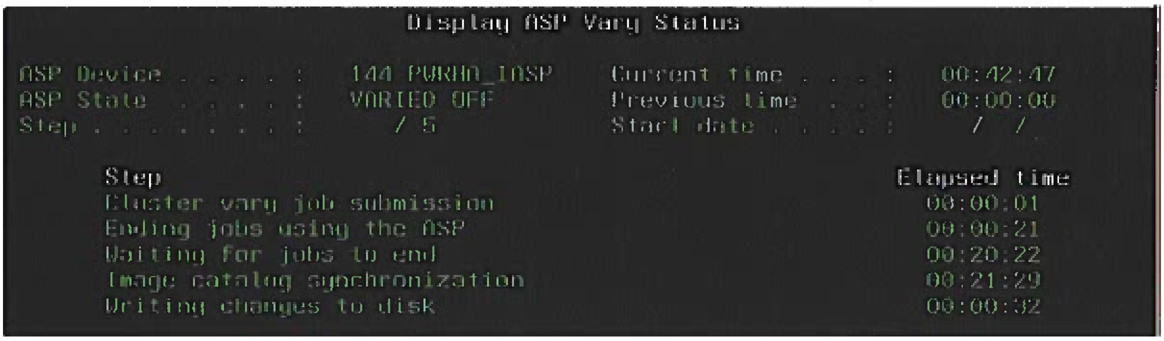
D). Check for jobs that are using the iASP, end any still present > WRKASPJOB

3/. **<u>On DR machine</u>** - CHGCRGPRI CLUSTER(PWRHA_CLU) CRG(PWRHA_CRG)

Initiates tasks:

Switchable IP's end on Prod (if any)
Vary off iASP on Prod
BU node promoted to Primary
Replication reversed
Vary on iASP on HA side
Starts switchable IP on HA side (if any)

4/. Use DSPASPSTS PWRHA_iASP on both sides to observe progress –

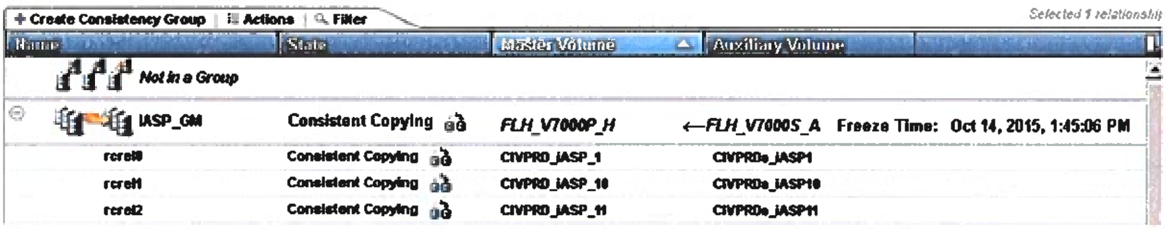


```
                         Display ASP Vary Status

ASP Device . . . . :   144 PWRHA_IASP     Current time . . . :   00:42:47
ASP State  . . . . :   VARIED OFF         Previous time  . . :   00:00:00
Step . . . . . . . :       / 5            Start date . . . . :     /  /

        Step                                           Elapsed time
        Cluster vary job submission                      00:00:01
        Ending jobs using the ASP                        00:00:21
        Waiting for jobs to end                          00:20:22
        Image catalog synchronization                    00:21:29
        Writing changes to disk                          00:00:32
```

5/. Look at the direction shown in V7000 Remote Copy | Consistency Group.

Look for the icon indicating the reversed direction (little arrow on Consistency Group heading

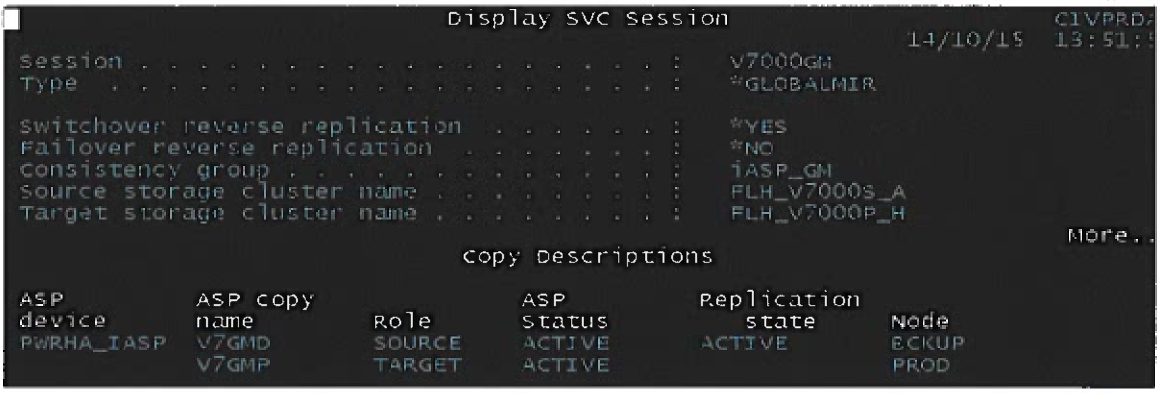
Line (iASP_GM) points to target)



Name	State	Master Volume	Auxiliary Volume	
Not in a Group				
IASP_GM	Consistent Copying	FLH_V7000P_H	←FLH_V7000S_A	Freeze Time: Oct 14, 2015, 1:45:06 PM
rcrel0	Consistent Copying	CIVPRD_iASP_1	CIVPRDe_iASP1	
rcrel1	Consistent Copying	CIVPRD_iASP_10	CIVPRDe_iASP10	
rcrel2	Consistent Copying	CIVPRD_iASP_11	CIVPRDe_iASP11	

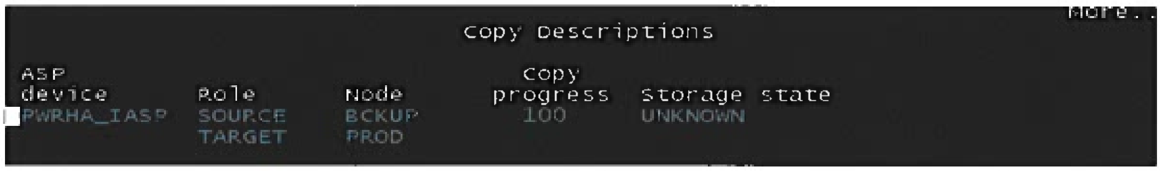
6/. DSPSVCSSN V7000GM, observe status of the PHA session. Backup node should have source role

in the recovery domain



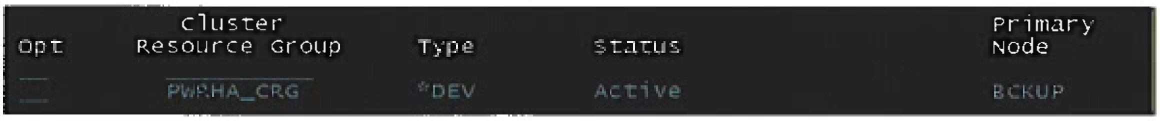
```
                          Display SVC Session                         CIVPRD
                                                              14/10/15  13:51:
 Session . . . . . . . . . . . . . . . . . . . . . :   V7000GM
 Type  . . . . . . . . . . . . . . . . . . . . . . :   *GLOBALMIR

 Switchover reverse replication  . . . . . . . . . :   *YES
 Failover reverse replication  . . . . . . . . . . :   *NO
 Consistency group . . . . . . . . . . . . . . . . :   IASP_GM
 Source storage cluster name . . . . . . . . . . . :   FLH_V7000S_A
 Target storage cluster name . . . . . . . . . . . :   FLH_V7000P_H
                                                                          More...
                          Copy Descriptions

 ASP          ASP copy                  ASP         Replication
 device       name         Role         Status        state       Node
 PWRHA_IASP   V7GMD        SOURCE       ACTIVE      ACTIVE        BCKUP
              V7GMP        TARGET       ACTIVE                    PROD
```

F11

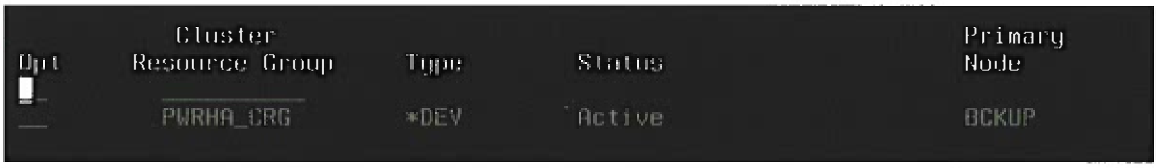


```
                          Copy Descriptions                               More...

 ASP                                    Copy
 device       Role         Node       progress     Storage state
 PWRHA_IASP   SOURCE       BCKUP        100        UNKNOWN
              TARGET       PROD
```

7/. WRKCLU – opt 9 Cluster resource groups - should show the node CIVPRDA is now primary node

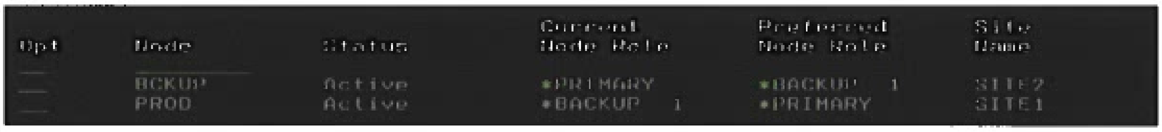


```
            Cluster                                                Primary
 Opt     Resource Group      Type           Status                   Node

 __        PWRHA_CRG         *DEV           Active                   BCKUP
```



```
           Cluster                                              Primary
 Opt    Resource Group      Type          Status                Node

 _
 __       PWRHA_CRG         *DEV          Active                BCKUP
```

Use option 6 against the CRG in the above display to show the recovery domain full detail:

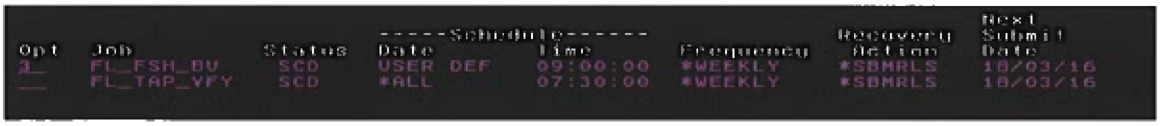


```
                                           Current           Preferred         Site
 Opt      Node           Status            Node Role         Node Role         Name

 __       BCKUP          Active            *PRIMARY          *BACKUP     1     SITE2
 __       PROD           Active            *BACKUP     1     *PRIMARY          SITE1
```

8/. Request a member of the Network Team to change the DNS “A” record bc.flhosting.co.uk from xx.xx.xx.xx (Handforth) to xx.xx.xx.xx (DC2).

(Directs the customer end users to DC2 instead of Handforth)

9/. On CIVFSHH - WRKJOBSCDE and hold FL_FSH_BU, so that the Flash Backup does not attempt to run when the iASP is varied off/switched to CIVPRDA.



```
                                                                                   Next
                                  -----Schedule------               Recovery       Submit
 Opt   Job            Status    Date          Time       Frequency     Action      Date
 3_    FL_FSH_BU       SCD      USER DEF    09:00:00     *WEEKLY     *SBMRLS     18/03/16
 __    FL_TAP_VFY      SCD      *ALL        07:30:00     *WEEKLY     *SBMRLS     18/03/16
```

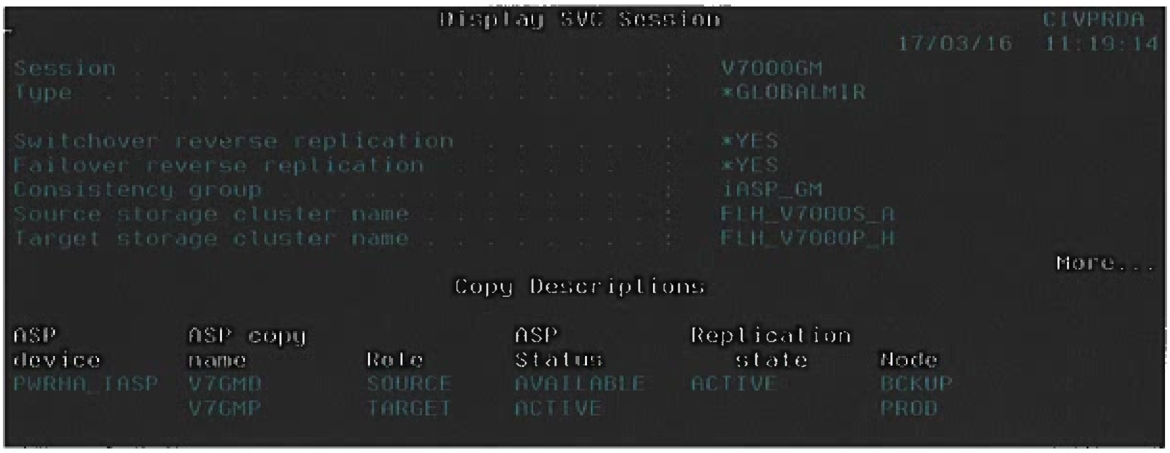
10/. Start up the customers system on the HA system > CALL QGPL/QSTRUP

(This submits - BOSSYS/RESETDAILY to start all customer jobs)

2. Planned Switch Back

1/. On BCKUP node -

DSPSVCSSN V7000GM - check working correctly. PROD node should have "TARGET" role.



```
                              Display SVC Session                    CIVPRDA
                                                            17/03/16  11:19:14
Session . . . . . . . . . . . . . . . . . . :   V7000GM
Type  . . . . . . . . . . . . . . . . . . . :   *GLOBALMIR

Switchover reverse replication  . . . . . . :   *YES
Failover reverse replication  . . . . . . . :   *YES
Consistency group . . . . . . . . . . . . . :   iASP_GM
Source storage cluster name . . . . . . . . :   FLH_V7000S_A
Target storage cluster name . . . . . . . . :   FLH_V7000P_H
                                                                       More...
                               Copy Descriptions

ASP          ASP copy                ASP         Replication
device       name         Role       Status         state       Node
PWRHA_IASP   V7GMD        SOURCE     AVAILABLE   ACTIVE         BCKUP
             V7GMP        TARGET     ACTIVE                     PROD
```

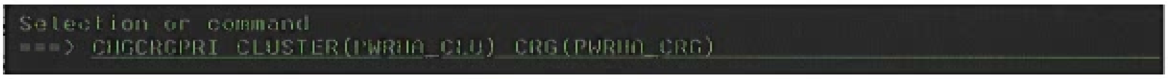
2/. Before starting the Switch, perform the following instructions on the HA partition:-

A). Sign-on as QSECOFR

B). End user jobs > CALL FL_PROD/FL_ENDJOB

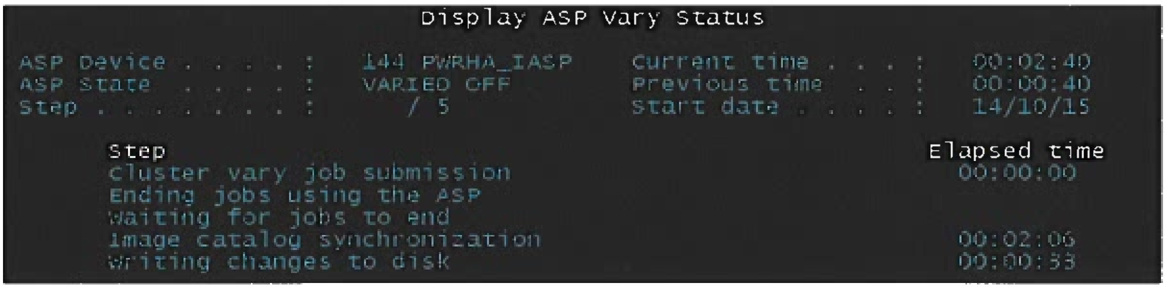
C). Check for jobs that are using the iASP, end any still present > WRKASPJOB

3/. CHGCRGPRI CLUSTER(PWRHA_CLU) CRG(PWRHA_CRG) on Production node, see below:



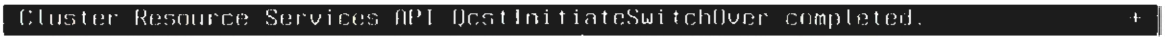
```
Selection or command
===> CHGCRGPRI CLUSTER(PWRHA_CLU) CRG(PWRHA_CRG)
```

4/. Use DSPASPSTS PWRHA_iASP on CIVPRDA to observe progress –



```
                         Display ASP Vary Status

ASP Device . . . . . :   144 PWRHA_IASP    Current time . . . :   00:02:40
ASP State  . . . . . :   VARIED OFF        Previous time  . . :   00:00:40
Step . . . . . . . . :         / 5         Start date . . . . :   14/10/15

      Step                                                   Elapsed time
      cluster vary job submission                              00:00:00
      Ending jobs using the ASP
      waiting for jobs to end
      image catalog synchronization                            00:02:06
      writing changes to disk                                  00:00:33
```

Message seen at bottom of CIVPRDH screen indicates success >

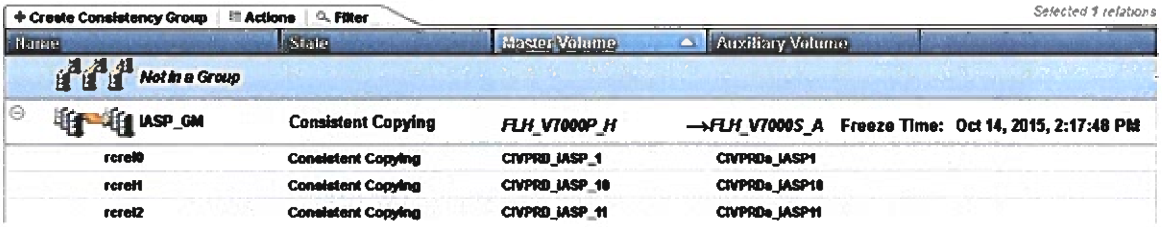


```
Cluster Resource Services API QcstInitiateSwitchOver completed.            +
```

5/. Look at the direction shown in V7000 Remote Copy | Consistency Group.

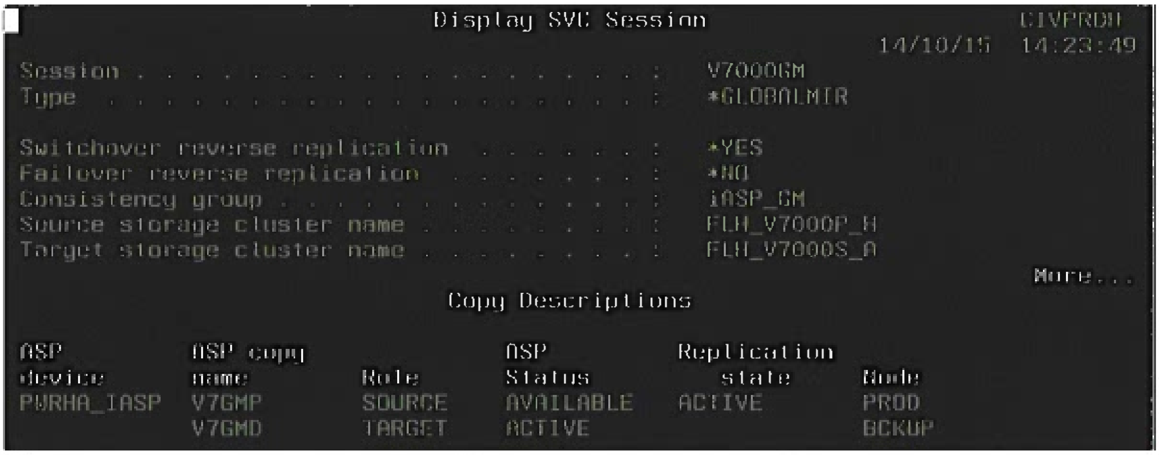
Look for the icon indicating the reversed direction (little arrow on Consistency Group heading

Line (iASP_GM) now points to FLH_V7000_A)



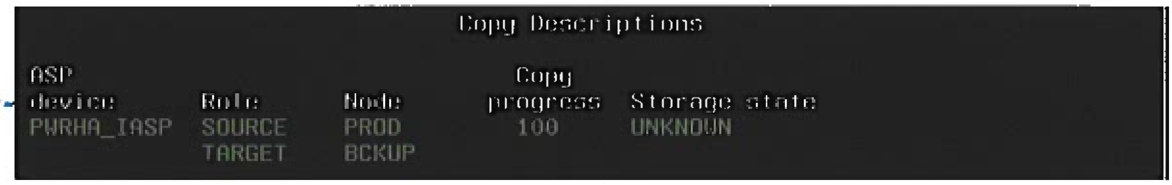
Name	State	Master Volume	Auxiliary Volume	
Not in a Group				
IASP_GM	Consistent Copying	FLH_V7000P_H	→FLH_V7000S_A	Freeze Time: Oct 14, 2015, 2:17:48 PM
rcrel0	Consistent Copying	CIVPRD_IASP_1	CIVPRDa_IASP1	
rcrel1	Consistent Copying	CIVPRD_IASP_10	CIVPRDa_IASP10	
rcrel2	Consistent Copying	CIVPRD_IASP_11	CIVPRDa_IASP11	

6/. DSPSVCSSN V7000GM, observe the SVC session status. PROD node should have "SOURCE" role:



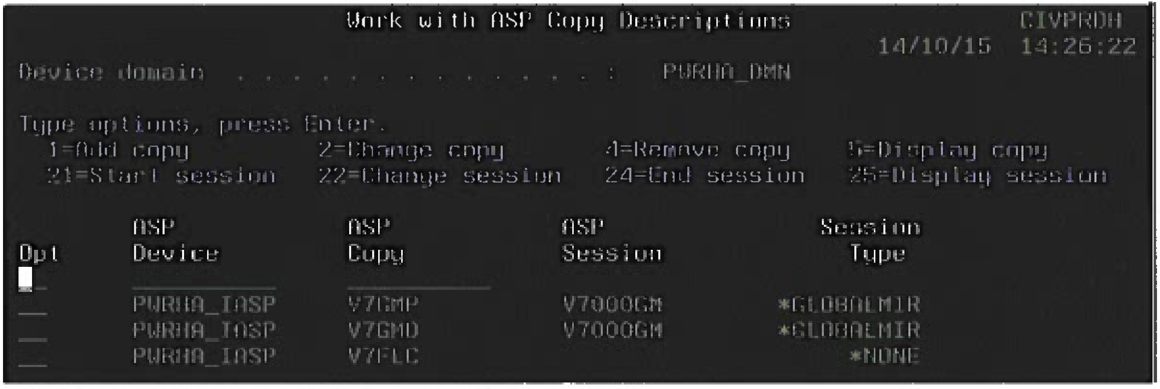
```
                          Display SVC Session                         CIVPRDH
                                                            14/10/15  14:23:49
 Session . . . . . . . . . . . . . . . . . . . . . :   V7000GM
 Type  . . . . . . . . . . . . . . . . . . . . . . :   *GLOBALMIR

 Switchover reverse replication  . . . . . . . . . :   *YES
 Failover reverse replication  . . . . . . . . . . :   *NO
 Consistency group . . . . . . . . . . . . . . . . :   iASP_GM
 Source storage cluster name . . . . . . . . . . . :   FLH_V7000P_H
 Target storage cluster name . . . . . . . . . . . :   FLH_V7000S_A
                                                                       More...
                           Copy Descriptions

 ASP          ASP copy                ASP          Replication
 device       name         Role       Status          state        Node
 PWRHA_IASP   V7GMP        SOURCE     AVAILABLE    ACTIVE          PROD
              V7GMD        TARGET     ACTIVE                       BCKUP
```

F11



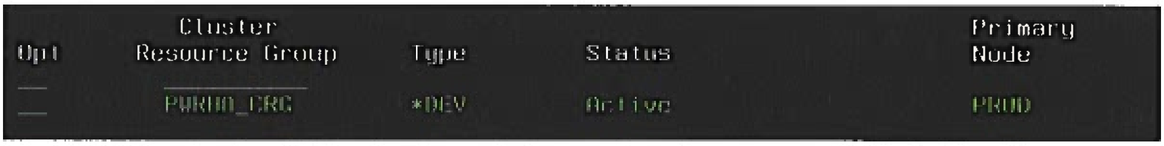
```
                           Copy Descriptions

 ASP                                  Copy
 device       Role       Node       progress   Storage state
 PWRHA_IASP   SOURCE     PROD          100      UNKNOWN
              TARGET     BCKUP
```

7/._WRKCLU option 10 - verify display as below:-



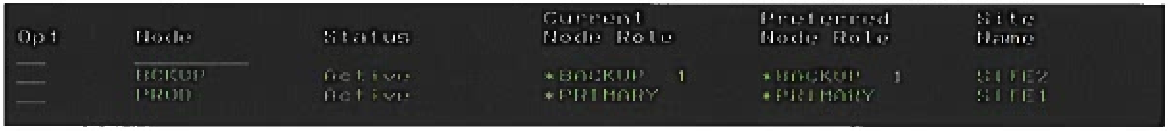
```
                      Work with ASP Copy Descriptions                 CIVPRDH
                                                            14/10/15  14:26:22
 Device domain  . . . . . . . . . . . . . . . :   PWRHA_DMN

 Type options, press Enter.
   1=Add copy          2=Change copy       4=Remove copy      5=Display copy
   21=Start session    22=Change session   24=End session     25=Display session

            ASP            ASP             ASP                 Session
 Opt        Device         Copy            Session               Type
 _
 __         PWRHA_IASP     V7GMP           V7000GM           *GLOBALMIR
 __         PWRHA_IASP     V7GMD           V7000GM           *GLOBALMIR
 __         PWRHA_IASP     V7FLC                                 *NONE
```

8/. WKCLU option 9 - verify Primary Node = PROD



```
                Cluster                                                       Primary
Opt        Resource Group       Type          Status                          Node
___
           PWRHA_CRG            *DEV          Active                          PROD
```

Use option 6 against the CRG in the above display to show the recovery domain full detail:

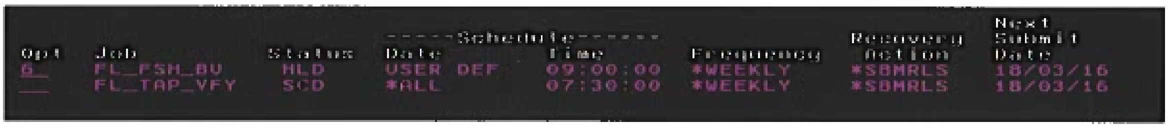


```
                                             Current           Preferred          Site
Opt      Node            Status              Node Role         Node Role          Name
___
         BCKUP           Active              *BACKUP     1     *BACKUP     1      SITE2
         PROD            Active              *PRIMARY          *PRIMARY           SITE1
```

9/. Request a member of the Network Team to change the DNS “A” record bc.flhosting.co.uk from xx.xx.xx.xx (DC2) to xx.xx.xx.xx (Handforth).

(Directs the customer end users to Handforth instead of Dc2)

9/. On CIVFSHH - WRKJOBSCDE and release FL_FSH_BU, so that the Flash Backup is reenabled.

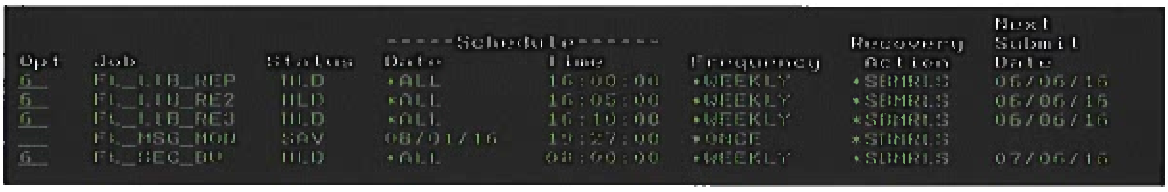


```
                                                                                      Next
                                  -----Schedule------                   Recovery      Submit
Opt    Job              Status    Date          Time         Frequency   Action        Date
6_     FL_FSH_BU         HLD      USER DEF      09:00:00     *WEEKLY     *SBMRLS       18/03/16
__     FL_TAP_VFY        SCD      *ALL          07:30:00     *WEEKLY     *SBMRLS       18/03/16
```

10/. Start up the customers system on the HA system > CALL QGPL/QSTRUP

(This submits - BOSSYS/RESETDAILY to start all customer jobs)

11/. Release 4 x Job Schedule Entries:-



```
                                                                                      Next
                                  -----Schedule------                   Recovery      Submit
Opt    Job              Status    Date          Time         Frequency   Action        Date
6_     FL_LIB_REP        HLD      *ALL          16:00:00     *WEEKLY     *SBMRLS       06/06/16
6_     FL_LIB_RE2        HLD      *ALL          16:05:00     *WEEKLY     *SBMRLS       06/06/16
6_     FL_LIB_RE3        HLD      *ALL          16:10:00     *WEEKLY     *SBMRLS       06/06/16
__     FL_MSG_MON        SAV      08/01/16      19:27:00     *ONCE       *SBMRLS
6_     FL_SEC_BU         HLD      *ALL          08:00:00     *WEEKLY     *SBMRLS       07/06/16
```

Switch History

Time recorded is for the full process not just the switch

Switch Date	Start Time	Completion Time	Switch Time	Comments
14/10/2015	11:36	12:20	44 mins	Switch PRD to BCKUP Resulted in “Indoubt” status
14/10/2015	14:12	14:26	14 mins	Switch Back
15/03/2016	12:58	13:31	33 mins	Switch PROD to BCKUP successful
17/03/2016	11:29	11:59	30 mins	Switch Back successful
09/06/2016	20:30	20:40	10 mins	Time corrected for small prob.
10/06/2016	01:48	02:02	14 mins	Clean Switch back