RCN Corporate Business Continuity Policy.

Authors:	Maxine Nunn
Role:	Performance, Risk and Assurance Manager
Version:	Version 7
Approved by:	RCN Executive Team
Approval date:	April 2021
Next review date:	November 2021

This policy is to be read in conjunction with the following operational documents, which are considered formal appendices to the document.

- Business Continuity instruction – "*Convening the Business Recovery Team*"
- Evacuation plans for individual RCN offices.
- HQ security action plan.
- IT Disaster recovery plan *(for IT use only).*
- Out-of-hours call out procedures for individual RCN offices.
- Personal Emergency Evacuation Plans (PEEPS) procedure.
- RCN Health & Safety policy.
- RCN Fire safety policy.
- RCN group IT policy.

Version control.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

This document is held on the RCN Intranet. Any paper copies of the document must be considered ‘uncontrolled version’. All updates and reissues of this document must be managed through the Performance, Risk and Assurance Manager.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Contents

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Note:

In an emergency, the staff holding the roles and job titles mentioned in this document may be unavailable. In such circumstances the role will be performed by the deputy identified in the local business continuity plan(s) - or will be assigned by the department's senior manager at the time.

The wide variety of scenarios that can lead to an emergency means it is unrealistic for this document to give detailed instructions on what to do in each and every situation. Instead, this document summarises RCN procedures and guidance that assist staff to manage and adapt as appropriate.

1. Policy and Scope.

1.1 Policy

The RCN aims to ensure an effective recovery of its services and return to business as usual after a significant business disruption or emergency. The organisation will put plans and processes in place to ensure recovery is achieved as effectively and efficiently as is possible in the circumstances.

The RCN is no different to other organisations where the threat of interruption to normal business presents a risk. Threats can come in many forms, at any location, and for an indeterminable duration. The impact on business operations can vary, with some departments able to operate a near normal service, whilst others suffer severe restrictions.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

The RCN recognises that business continuity planning (BCP) increases organisational effectiveness when managing an emergency; hence, the following responsibilities are recognised;

1.1.1 The Executive Team collectively commit to business continuity planning and its implementation, providing strategic direction and commitment to the organisation's business continuity activities.

1.1.2 When the Chief Executive and General Secretary is unavailable the Director Northern Ireland will always deputise. [1]

1.1.3 The Executive Team collectively recognise the need for a core team to oversee any emergency, and will therefore ensure a Business Recovery Team is put in to place to provide corporate-level decision-making following a critical incident.[2]

1.1.4 The Business Recovery Team will ensure that robust communication networks are in place to allow their decision-making to take place in situations where the emergency means usual communication methods are compromised or non-existent.

1.1.5 Executive Directors will ensure that their Countries, Regions, and Departments have appropriate business continuity plans in place, will test them in accordance with the annual plan and report lessons learned to the Executive Team.

1.1.6 Executive Directors will ensure staff are aware of business continuity and disaster recovery arrangements in their Countries, Regions, and Departments.

1.1.7 The Executive Team, plus other key members of the Business Recovery Team will annually appraise the organisation's training requirements to ensure staff understand the organisation's BCP policy and requirements.

1.1.8 The Governance Planning Manager manages upkeep and review of this policy.

1.1.9 All staff are responsible for understanding, and complying with, the local and corporate BCP requirements.

1.2 Scope.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

This policy focuses on four major activities:

- Recognising and understanding an emergency.
- Our immediate response to the emergency.
- How to recover Estates or Information capabilities that have been damaged.
- How to ensure the business continues with its day-to-day work.

Figure 1 captures the chronology of these four categories.

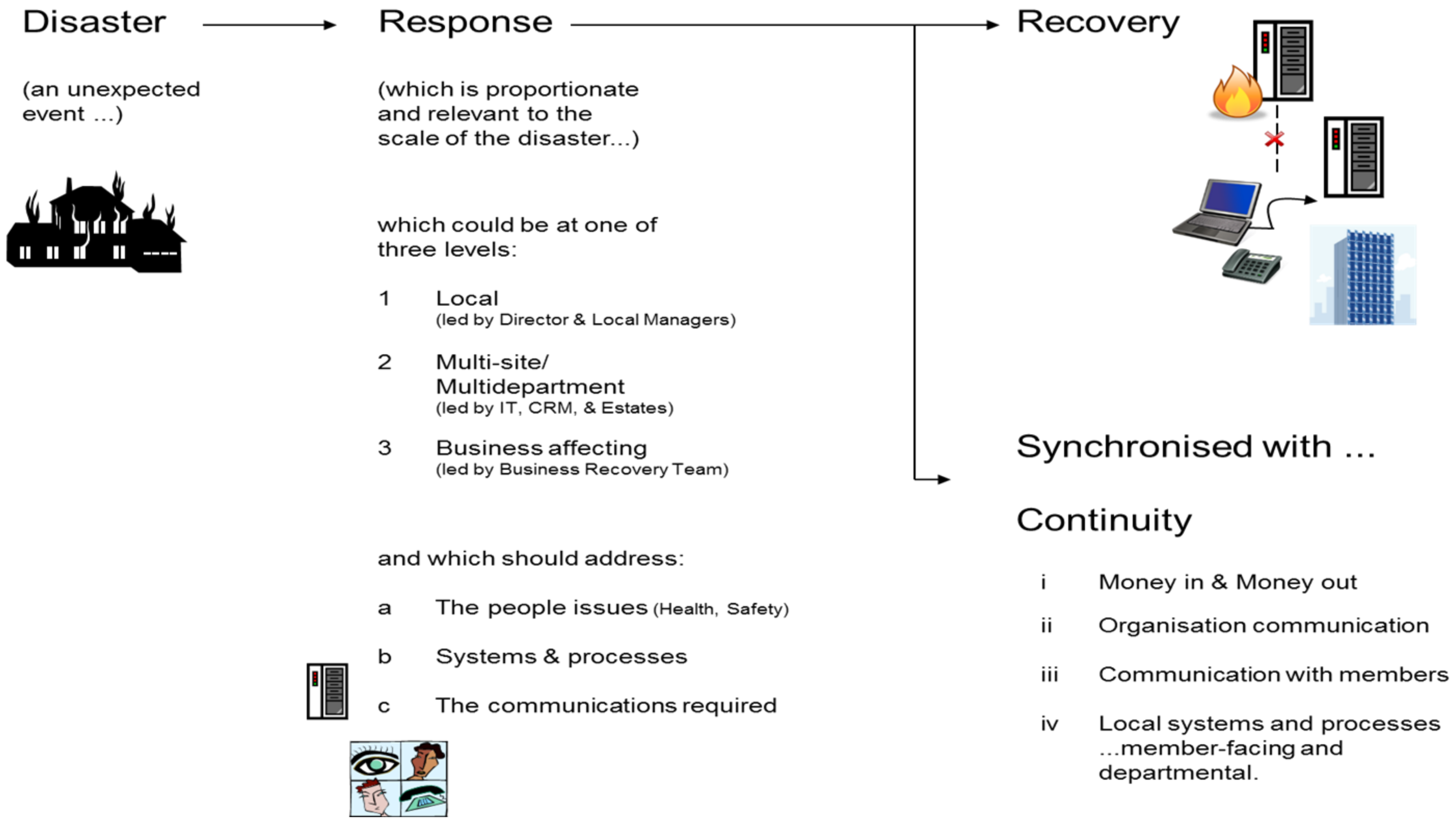
This document provides an overview of each category, and identifies corporate and local processes to manage them.

As mentioned, the wide variety of scenarios that can lead to an emergency means it is unrealistic for this document to give detailed instructions on what to do in each and every situation. Instead, this document summarises RCN procedures and guidance that assist staff to manage and adapt as appropriate.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Figure 1: An overview of the four significant BCP categories.



Disaster

(an unexpected event …)

Response

(which is proportionate and relevant to the scale of the disaster…)

which could be at one of three levels:

1 Local
(led by Director & Local Managers)

2 Multi-site/ Multidepartment
(led by IT, CRM, & Estates)

3 Business affecting
(led by Business Recovery Team)

and which should address:

a The people issues (Health, Safety)

b Systems & processes

c The communications required

Recovery

Synchronised with …

Continuity

i Money in & Money out

ii Organisation communication

iii Communication with members

iv Local systems and processes …member-facing and departmental.

2. Governance and Ownership.

2.1. The Executive Team take collective responsibility for embedding the management of business continuity at both an organisation-wide level and at the level of individual Countries, Regions, and departments.

2.2. A sub-group of the Executive Team form part of the Business Recovery Team (alongside other key staff). This team will convene following the announcement of an emergency, as detailed in Figure 2.

2.3. Business Recovery Team members are listed in the document "RCN Business Continuity instruction - Convening the Business Recovery Team" - alongside information on individual roles and responsibilities.

2.4. At Country, Regional, and Cardiff Gate office locations, the responsibility for BCP processes, decision-making, and management lies with the senior manager at that office at the time of the emergency (unless directed otherwise by their Executive Director). The process to be followed in an emergency is defined in each location's BCP action plan.

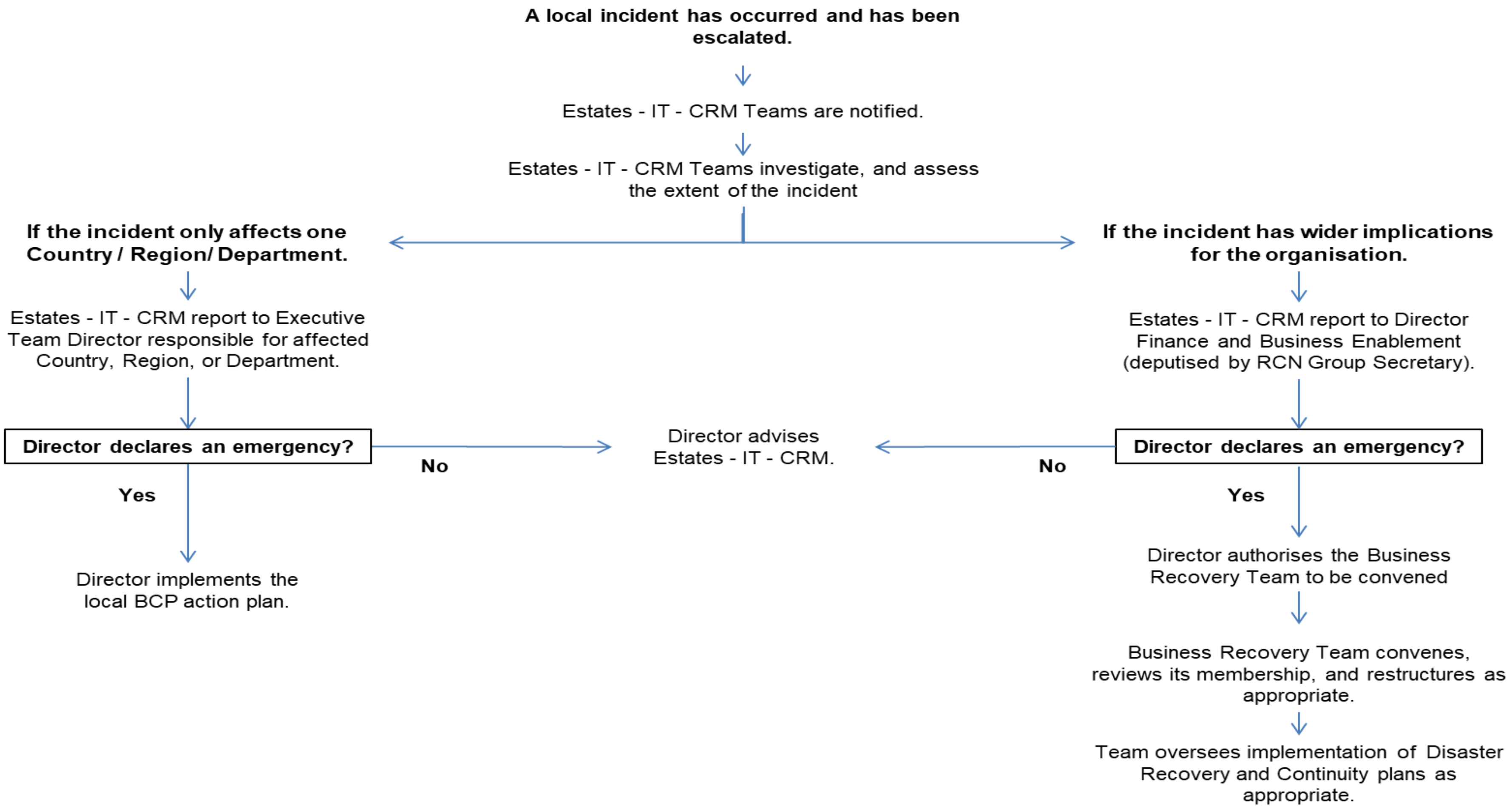
2.5. Each location's action plan will explicitly state the level of autonomy that local managers are expected to assume if the emergency scenario means Executive Team guidance is unavailable.

2.6. It is recognised that industry standards exist that allow formal accreditation of Disaster Recovery and Business Continuity processes e.g. British Standards, ISO. The RCN will remain abreast of developments in external standards and industry best practice, and continue to use those as guidelines for managing business continuity. However, the RCN will not seek formal accreditation to those external standards: instead, regular internal audits will highlight any shortcomings against industry norms.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Figure 2: Decision-tree for confirming emergency status.



A local incident has occurred and has been escalated.

Estates - IT - CRM Teams are notified.

Estates - IT - CRM Teams investigate, and assess the extent of the incident

If the incident only affects one Country / Region/ Department.

Estates - IT - CRM report to Executive Team Director responsible for affected Country, Region, or Department.

Director declares an emergency?

No

Yes

Director implements the local BCP action plan.

Director advises Estates - IT - CRM.

If the incident has wider implications for the organisation.

Estates - IT - CRM report to Director Finance and Business Enablement (deputised by RCN Group Secretary).

Director declares an emergency?

No

Yes

Director authorises the Business Recovery Team to be convened

Business Recovery Team convenes, reviews its membership, and restructures as appropriate.

Team oversees implementation of Disaster Recovery and Continuity plans as appropriate.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

3. Health, Safety, and Emergency Services.

3.1 The RCN Health & Safety policy[1] notes that the organisation has provision for;

- Fire prevention, through inherent fire safety, employee awareness and good housekeeping.
- Evacuation procedures for emergencies.
- Fire detection and extinguishing systems.
- Firefighting at key locations, through trained employees.
- Emergency Officers and Fire Marshals at all staffed premises.
- Incident management processes.

3.2 Guidelines for contacting Emergency Services are published in emergency evacuation plans held at each RCN location. At Cavendish Square HQ these plans are owned and maintained by the Estates Team - all other plans are owned and maintained by the Executive / Regional / Department Director resident at that location (for freehold buildings) or the building Landlord (for leased buildings).

4. Responding to the incident.

The immediate response by local managers will depend upon the type and scale of incident.

Some incidents may lead to limited (or no) staff able to attend the building e.g. virus outbreak, lack of transport.

Other situations may directly affect the availability of IT networks or access to business information e.g. network connectivity, Customer Relationship Management system (CRM), email.

Additional causes may directly affect the building itself: e.g. fire, loss of power.

[1] Health and Safety Policy. Version 2.0. Stored on RCN Intranet.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

It is important that managers recognise the impacts of an emergency may be significantly worse in other parts of the organisation, and should react accordingly, seeking status reports on the wider impacts where necessary.

Disaster recovery and business continuity plans may need to be escalated if a local incident escalates beyond the control or experience of the employees at the scene.

4.1 Escalating an IT affecting issue (e.g. cyber-attack).

The organisation's growing reliance on remote working means that, increasingly, staff IT requirements are not linked to an office or a geographic location. Consequently, the effects of an incident such as cyber-attack can be felt far beyond the office.

All Cyber Security Incidents must be reported to the IT Service Desk in the usual way of logging an IT incident. The Service Desk will log the Cyber incident detail and notify the Head of IT and Data Protection Officer of the incident.

Once identified, a Cyber Incident Response Team will use the RCN IT Service Desk to log and track the Cyber Security Incident and as appropriate, take steps to investigate, escalate, and remediate the Incident.

The Head of IT or Data Protection Officer will determine if Law enforcement should be informed and will continue to liaise with the appropriate authorities throughout the incident. The Head of IT or Data Protection Officer will determine if the Cyber insurance claims hotline should be contacted to engage further support in managing and responding to a Cyber incident.

4.2 Escalating a staff-affecting incident (e.g. epidemic, failed transport).

Disaster Recovery and Business Continuity plans may need to be brought in to effect if an external incident -

- affects the ability of RCN staff to travel to work
- leads to levels of staff sickness that reduce the organisation's effectiveness

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

- leads to absence of staff providing essential infrastructure support (e.g. Estates or IT staff supporting infrastructure required by the rest of the organisation).

In all such instances, local managers must contact the IT Operations Manager and/or Head of Estates in order to quantify and qualify the extent of any service disruption and to appraise alternative solutions.

If the problems raised by staff absence cannot be resolved within Estates and Information Technology teams, the Director Finance and Business Enablement (deputised by RCN Group Secretary) should be informed and can consider escalating the situation to the Business Recovery Team (see section 5.1).

4.3 Escalating incidents when the Customer Relationship Management system (CRM) becomes unavailable.

Local managers must contact their CRM Power User first. The Power User is then responsible for raising a call with the IT Service Desk, which will alert both the IT Operations Manager and the CRM Team Lead.

The IT Operations Manager and CRM Lead will assess if the root cause lies with the IT infrastructure or the CRM itself. They will also decide if the incident should continue to be managed locally, or if the situation should be escalated to a formal emergency (see Figure 2).

The IT Operations Manager and CRM Team Lead will contact the Communications team to discuss what information should be communicated within the organisation and how.

4.4 Escalating an information affecting incident (e.g., no access to IT network, email is unavailable).

Local managers must contact the IT Operations Manager by raising a call with the IT Service Desk.

The IT Operations Manager will decide if the incident should continue to be managed locally, or if the situation should be escalated to a formal emergency (see Figure 2).

The IT Operations Manager will contact the Communications team to discuss what information should be communicated within the organisation and how.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

4.5 Escalating a building-affecting incident.

For example:

- A fire or similar incident that demands intervention of the emergency services.
- A flood or similar incident that requires intervention of outside specialists.
- A Health & Safety breach (asbestos, chemical spillage, water contamination) that requires the intervention of the RCN Health & Safety manager.

Once made aware of the situation the Estates Team will take the lead on these types of incident, working alongside the Health & Safety manager, local management, and appropriate external specialists. The Head of Estates and the IT Operations Manager will consider the appropriate action to be taken and will decide if the incident should continue to be managed locally, or if the situation should be escalated to a formal emergency (see Figure 2).

Irrespective of the outcome of that decision, the Head of Estates and the IT Operations Manager will contact the Communications team to discuss what information should be communicated within the organisation and how.

4.5.1 Escalating building-affecting incidents in working hours.

During working hours the Head of Estates and IT Operations Manager (or their deputies) must be contacted, and informed of the scope and scale of the situation. The IT Operations Manager is contacted via the IT Service Desk (as detailed in the IT Disaster Recovery Plan); the Head of Estates is contacted using their RCN landline or mobile telephone number.

4.5.2 Escalating building-affecting incidents outside working hours.

The procedure for out of hours problems is that the building's contracted key holding service will contact whoever they have been advised is the local RCN member of staff responsible for the office. This might be the person located closest to the office rather than a Director. The local staff member will make the initial assessment of the scope and scale of the

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

problem - and then contact the Head of Estates and/or IT Operations Manager if the problem demands escalation.

It is recognised that (i) escalating a problem out-of-hours is more difficult and (ii) to do so immediately could be inappropriate (there may be no effective action the RCN can take until the following working day).

Consequently, the decision to escalate an incident out-of-hours depends on local management judgement of the scope/scale of the threat: there may be instances when the most appropriate action is to wait until the next working day.

In summary, out-of-hours cover will be managed at 'best endeavours' with staff call-out and communications set at an appropriate level for the location concerned. For example, London HQ has implemented a formal call-out process where a member of the Estates team is notified in the event of a significant incident.

4.6 Evacuating a building.

Emergency evacuation plans are held at each RCN building, although different document formats exist depending upon the building ownership (i.e. owned vs. leased), and building occupancy (i.e. single tenant vs. multiple tenant).

All evacuation procedures are audited annually as part of the Fire Safety Risk Audit. Guidance on building evacuation procedures is available within the RCN Fire Safety Policy document.

4.6.1 Evacuating Cavendish Square HQ.

The response to an incident will follow the Emergency Evacuation Plan owned by the RCN Estates Team.

4.6.2 Evacuating Country & Regional offices (including Cardiff Gate).

Building evacuation will follow the local processes: evacuation plans for buildings are owned and managed by the local/country/regional directors.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

5. Formally announcing an emergency, and convening the Business Recovery Team.

5.1 Once escalated by the Head of Estates, IT Operations Manager, or CRM Lead, the responsibility for confirming that an incident warrants 'emergency' status lies with the Director Finance and Business Enablement or their assigned deputy (RCN Group Secretary).

5.2 The Director Finance and Business Enablement will assess the severity of the incident and its effect on the organisation before deciding the extent to which the situation should be escalated.

It may be that the situation can be contained and managed locally; alternatively, the situation may require the involvement of the Business Recovery Team, other RCN staff, and external agencies.

6. Activity once an emergency is formally declared.

Once an emergency has been declared, several areas of activity require managing concurrently. Figure 1 defines these areas as people, systems, processes, and communications. These areas may also require managing across multiple locations and/or between more than one group of people.

By default, it is the responsibility of the senior manager at the emergency site to instigate local emergency procedures (unless the procedure specifically states an alternative employee).

Note that the processes at some RCN locations contain minor variations and use local document names e.g. Critical Incident Plan, Major Incident Plan, and Local Action plan. However, they all aim to define the roles, responsibilities, and priorities to be enacted in the short-term by the local staff.

6.1 When a building is unavailable or evacuated; however, staff are available to work.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

If the emergency forces a building to become unavailable, the organisation must manage not only the affected staff at that location, but also any visitors planning to travel to the location.

6.1.1 Decision to send staff home or relocate.

When the Business Recovery Team has convened its members will liaise with local management at the emergency site to discuss the next steps to be taken. This could involve re-entering parts of the site, possible temporary relocation elsewhere, or the need to send staff home.

If the Business Recovery Team is unavailable, the senior manager at the emergency site is authorised to make the decisions (taking advice of the Head of Estates, Head of Health and Safety and IT Operations Manager, wherever possible).

In some instances, a department's teams are co-located with regional / Cardiff Gate office staff. The senior manager with responsibility for the regional office will act as surrogate head of those teams, and the team members should follow any local instructions for building evacuation, office closure, etc.

6.1.2 Notifying visitors intending to travel to an affected RCN location.

Both the closure of an RCN office, or the lack of people to staff it, will affect planned events or meetings. It is important that the attendees of any planned events be notified of the emergency to prevent unnecessary travel and disruption on their part.

- London HQ meeting rooms. The conference services team use an electronic, web-based room booking system. In an emergency, the information will be accessed remotely.

- Other RCN locations. All England regional offices maintain a dedicated Microsoft Outlook calendar that manages visitor information and room bookings at those offices. In the event of an emergency, this information will be remotely accessed over the RCN network, and visitors informed of the situation.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

- RCN Events Team. Contact details for attendees at RCN Events will be accessed from the RCN Membership Database by the Marketing department's Events team. The Events team will take responsibility for notifying attendees of the emergency.

6.2 When buildings and infrastructures are unaffected, however staff are unavailable.

6.2.1 Where staff sickness/absence leads to an emergency (i.e. insufficient staff available for the business to function), local management should work with the Business Recovery Team to investigate and implement alternative resources. The local Action Plan will identify critical functions that may need reprioritising and rescheduling.

6.2.2 Where a failed transport network means that healthy staff are unable to attend their usual workplace, the local BCP Action Plan will identify the department capability to work remotely, and the supporting infrastructure needed by staff to work away from their office (e.g. remote access to email, relocation to alternative premises).

7. Recovering from the effects of the incident.

Disaster recovery is predominantly the responsibility of two RCN departments – Estates and Information Technology. These departments are responsible for the restoration of critical corporate/local infrastructures in the aftermath of an incident.

The means by which these departments will restore the organisation's key infrastructures are summarised below; more detailed information and processes are held within each department's own documentation.

7.1 Disaster Recovery - Information Technology.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

The recovery of our IT infrastructure is led by the Information Technology (IT) team, who are responsible for providing core information and communication technology, and data processing across the organisation.

The continuity of systems and business processes will be assured by incorporating resilience and by disaster recovery and contingency planning.

The IT Department has adopted a variety of controls to ensure high availability of Corporate Critical systems using methods such as:

Backup and restore procedures, Offsite storage, Cyber Security Controls, Antivirus software and procedures, Environmental controls, and Physical and logical controls.

The IT team publish Disaster Recovery Plans that address these topics, and identify how Corporate Critical functions will be recovered following an emergency. The current Corporate Critical IT functions are listed in the table below.

System	**Maximum Restoration time**
Email	1 day
CRM	1 day
Electronic files	1 day
Case Management System	1 day
Direct Debit	2 days
eBis	2 days
Payroll	1 day

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

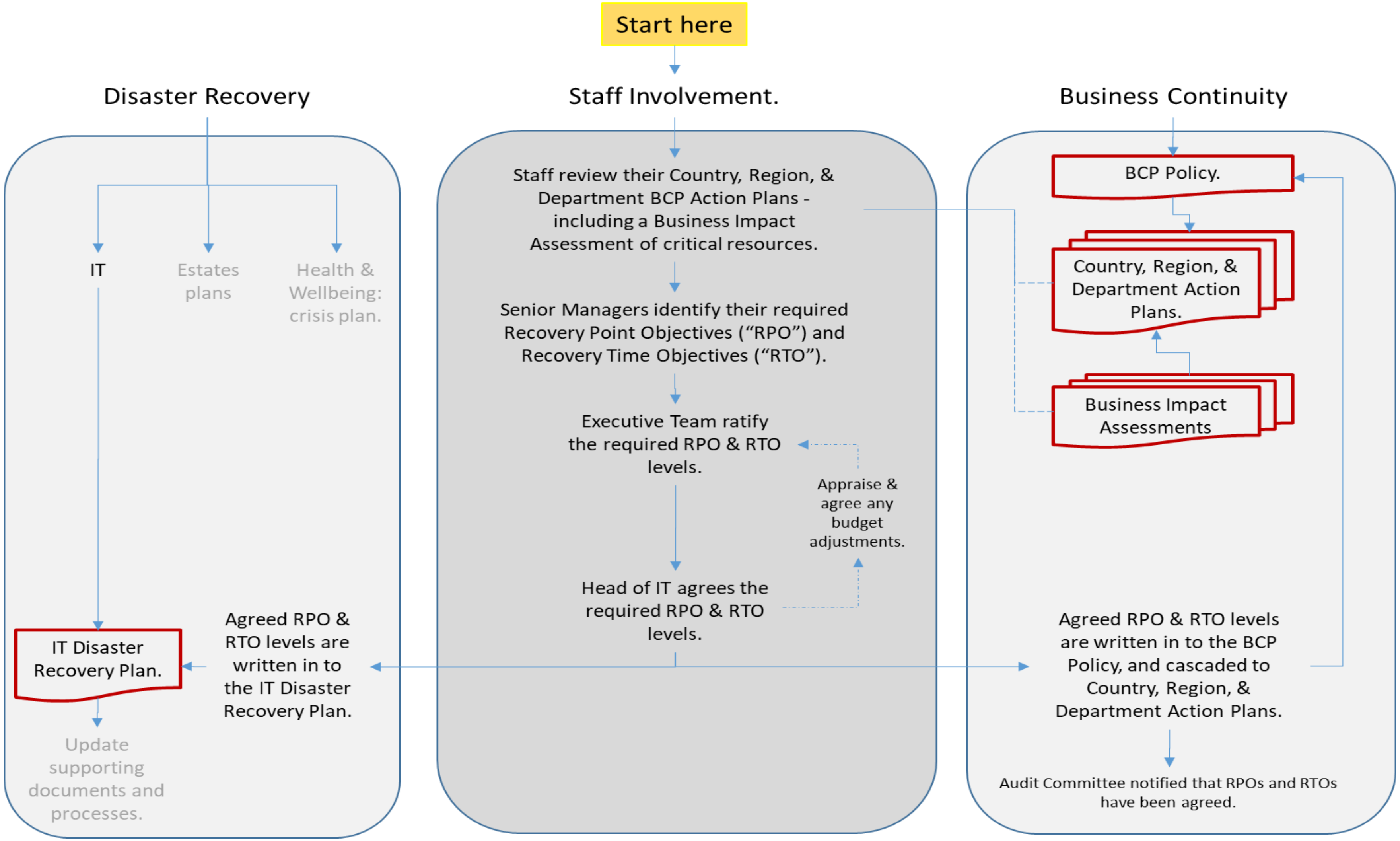
OpenHR	1 day
Telephones	Dependent on fault. In most cases, a scaled service within 30 minutes would be offered.
RCN Website	Maximum downtime currently estimated at 30-hours.

Critical IT functions should be identified using the process depicted in Figure 3.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Figure 3: Conducting Business Impact Assessments and updating critical objectives.



Start here
Disaster Recovery
Staff Involvement.
Business Continuity
IT
Estates plans
Health & Wellbeing: crisis plan.
Staff review their Country, Region, & Department BCP Action Plans - including a Business Impact Assessment of critical resources.
Senior Managers identify their required Recovery Point Objectives ("RPO") and Recovery Time Objectives ("RTO").
Executive Team ratify the required RPO & RTO levels.
Appraise & agree any budget adjustments.
Head of IT agrees the required RPO & RTO levels.
BCP Policy.
Country, Region, & Department Action Plans.
Business Impact Assessments
IT Disaster Recovery Plan.
Agreed RPO & RTO levels are written in to the IT Disaster Recovery Plan.
Update supporting documents and processes.
Agreed RPO & RTO levels are written in to the BCP Policy, and cascaded to Country, Region, & Department Action Plans.
Audit Committee notified that RPOs and RTOs have been agreed.

[1] unavailable is anytime when the CE & GS is uncontactable to make or agree a decision relating to business continuity of the organisation.

[2] Details are in the RCN Business Continuity instruction - Convening the Business Recovery Team: stored on the RCN Intranet and within the secure area of emergency information webpage www.support.rcn.org.uk

Note: the full suite of IT systems used by staff and members must be considered when completing a Business Impact Assessment - not only the systems familiar to the assessor.

For example, at the time of writing the organisation is known to use;

Aderes .
AdvicePro
AdvicePro Money
Appraisals system
Barclaycard portal
ChqFlow
Case Management
Click Travel
CoreNet
Customer Relationship Manager
Design portal
Dot Digital
DSE System
eBis
Email
eVault Archive
Experian
Intranet
ModGov
OpenAccounts
OpenHR
Skype
Social Media
Talentlink
Talentlink LMS
Verint
Website

It is important to note that IT Disaster Recovery plans do not include arrangements for small applications that are owned and supported by local users. Disaster Recovery will be provided for such systems on a ‘best endeavours’ basis and only when critical systems have been restored.

Staff and members using such local applications or personal equipment must be made aware of the implications of using such unsupported technologies. Whenever they are using their own equipment, they should always try to use the RCN Terminal Server Access and limit their access to sensitive RCN data. Storage of RCN data on any personal devices during an outage should be limited to that which is essential and it should be removed at the earliest convenience.

7.2 Disaster Recovery - CRM.

As well as the CRM system, we maintain a CRM '*DR solution'*. The CRM *DR solution* duplicates what the CRM does, with the latest information from the CRM being backed up every night. In the event of a CRM problem, the information available through the CRM *DR solution* will be as current as the day before the issue occurred.

The Business Recovery Team will decide whether to invoke the CRM *DR solution*, which should typically be available to staff within 24 hours of that decision being made.

Any information that is put into the CRM *DR solution* will be automatically transferred back into the actual CRM once it has been restored.

7.3 Disaster Recovery – Cyber Attack.

The IT team maintain a Computer Security Incident Response Plan that governs the RCN's general response, documentation and reporting of network and computer-based IT Security incidents, such as theft, intrusion, denial of service, and unauthorised access.

The purpose of the plan is to protect the integrity, availability and confidentiality of the RCN's confidential and proprietary information, to prevent loss of service and to comply with legal and regulatory requirements.

In the event of a cyber incident, the Head of IT or Data Protection Officer will work in conjunction with management, the Information Technology department and others to establish a Security Incident Response Team appropriate to respond to a specific incident or threat.

The Head of IT or Data Protection Officer will inform the Director Finance and Business Enablement and the RCN Group Secretary of the incident outlining the nature of the incident.

The Head of IT or Data Protection Officer will also be responsible for communicating the Incident to appropriate personnel and maintaining contact, for the purpose of update and instruction.

Alongside this plan, the RCN takes out a specialised cyber-security insurance policy, covering Legal Services, IT Services, Data Restoration, Reputational Protection Services, Notification Costs; and Credit Monitoring and ID Monitoring.

7.4 Disaster Recovery - Estates.

The Estates team are responsible for numerous offices of various sizes throughout the UK, with the offices providing a working environment and associated meeting rooms. In addition, the Estates team are responsible for the maintenance of the organisation's mechanical and electrical systems, building security, and management of HQ conference services.

The actions taken by the Estates team to restore any damaged infrastructure are dictated by two questions that need to be asked once the root cause of the incident has been stabilised;

- What is the condition of the infrastructure once the cause of damage has been contained? e.g. is the office accessible, safe, powered, watered, and available for use (albeit in a limited capacity).
- What infrastructure requirements need to be provided to allow business to continue? e.g. the access to alternative RCN accommodation or access to other accommodation - as defined in the departmental Business Impact Analysis documents.

The answers to these questions allow the Estates Team to plan the degree of activity necessary to restore the damaged infrastructure, versus resource necessary to provide alternative infrastructures needed to ensure business continuity.

8. Business Continuity during and following the incident.

Business continuity plans are instigated alongside the work to rebuild any affected Estates and IT infrastructure. The continuity plans allow the organisation to adapt its ways of working in the medium and long-term to allow services to resume and continue as quickly as possible.

There are four core elements to the RCN's Business Continuity plans.

- The financial security of the organisation i.e. maintaining the movements of money into and out of the organisation.
- Organisation communication
- Communication with members
- The local systems and processes (member-facing and departmental) that allow the organisation to maintain its services.

The means by which these are managed are listed below;

8.1 Continuity of core functions.

8.1.1 Financial security.

All the organisation's critical financial systems are electronic, and form part of the disaster recovery plan for the Information Technology team. However, the nature of the emergency may mean that financial systems cannot be diverted or restored in the short-term and consequently a work-around structure is required.

The Director Finance and Business Enablement and the IT Operations Manager are both members of the Business Recovery Team; the CRM Lead will be amongst the key personnel that the recovery team has at its disposal. Consequently, any impact on the effective financial running of the organisation can be assessed by them almost immediately, and workarounds put into place. Examples include;

8.1.1.1 EBis Finance expenses system. This is a resilient system with a failover provision between two independent servers. A manual intervention will allow the system to be restored in a few minutes.

8.1.1.2 Direct Debit system for membership and RCNI subscriptions, and RCN Foundation donations. Systems are in place to allow BACS processes and tasks to be performed at Cardiff Gate (where this activity normally occurs) or from any other RCN office or remotely, providing the necessary RCN IT networks are in place and the relevant personnel available. In the event of CRM system failure, retrieval and restoration of the system should be within 24 hours of the Disaster Recovery plan being invoked.

8.1.1.3 Payroll System. Tests have confirmed that PBS can access our system and run our payroll file in the event of an incident (this assumes the London or Cardiff network is functional).PBS will then run the payroll file. Note, that in addition it may be possible for PBS to submit BACS at the same time.

8.1.1.4 Not all RCN offices manage their Finance functions using the HQ-based team. If an emergency leads to the unavailability of those local finance roles, cover will be provided by the HQ team for a short period, at an appropriate level, and under the guidance of the Director, Finance and Business Enablement.

Conversely, if HQ finance staff are unable to get to the HQ building, key staff will be redirected to other RCN offices to use the computers at those locations. However, the IT team will have to reconfigure those temporary finance computers, to allow finance staff to access Open Accounts and other finance-specific software packages.

A similar problem will exist if finance staff work remotely from non-RCN locations; their remote computers will not have the full suite of financial applications loaded on them.

8.1.1.5 If HQ finance staff are unable to work (through sickness), ABS will have to be contacted (i) to assess if they have resources available to assist the RCN workload (ii) to ask them to reconfigure existing RCN non-finance systems to allow finance work to be done by Country Finance Teams (N. Ireland, Wales, Scotland ...).

8.1.2 Continued provision of Estates infrastructures.

If a building has been damaged or is otherwise unavailable for use, the Estates Team will manage its repair/closure as part of their Disaster Recovery processes. However, in parallel with this activity there may be a need to provide alternative accommodation to staff and members as an interim measure. Departmental Business Impact Analyses identify departmental needs in the short, medium, and longer-term, and the Estates Team will liaise with senior managers of any affected departments to negotiate a practical and appropriate solutions. In particular, it is important that managers at affected locations identify which staff and resources require rapid relocation - enabling the Estates Team to implement temporary measures if necessary.

RCN Estates offer several levels of organisational resilience:

- RCN properties are mostly located in neighbouring geographical areas, and the Estates Team has considered how a disaster in one location might allow the possibility to relocate to an adjacent location. In a site-affecting emergency, the Estates Team will discuss the feasibility of such relocations with the appropriate Directors (Country, Regional, HQ, and Cardiff Gate).

- The RCN Estates Team has good industry contacts, specifically with our retained property agency (HMC). Liaising with the agency allows us opportunity to find alternative locations for the short/medium term.

- The RCN Estates Team has links to organisations that lease business accommodation (e.g. Regus), and will approach such organisations if other options are unavailable to the organisation.

8.1.3 Provision of Human Resources support to affected Country offices.

Not all RCN offices manage their HR functions using the HQ team. If an emergency leads to the unavailability of those HR functions, the roles will be covered by the HQ team for a short period, at an appropriate level and under the guidance of the Business Recovery Team.

8.2 Continuity of local functions.

Local Action Plans and/or Business Impact Assessments (BIA) have been published by every department; see paragraph 7.1 for details. These documents identify the impacts to the business when an incident leads to loss or interruption of a department's ability to function.

In the aftermath of an emergency, these documents will be used by local management and the Business Recovery Team to assess local requirements over and above the critical corporate functions being restored.

The Business Recovery Team will use the contents of a Business Impact Analysis / Action Plan document to appraise what services and resources require rebuilding, and the priority and timescales of those rebuilds. This will be negotiated in collaboration with the management team at the affected location.

More importantly, the documents allow the Business Recovery Team to investigate alternative sources of resource and infrastructure to mitigate the effect any disaster has had on resources and service capability.

The Action Plans are available to the Business Recovery Team by logging in to the RCN's remote Emergency Information website www.support.rcn.org.uk.

Upkeep of these documents is the responsibility of Country Directors, regional Directors, and Heads of departments. Owners will update their documents whenever local working methods or infrastructures dictate it to be appropriate; notwithstanding this, all documents must be reviewed annually.

When a BCP-related document is updated, the local manager is responsible for notifying the Governance Planning Manager, who will upload copies of Action Plans to the Emergency Information website - where they can be accessed by the Executive Team and Business Recovery Team.

8.3 Continuity of RCNi and RCN Foundation.

8.3.1 The RCN Foundation stores its electronic file data on the RCN Information Systems. Following an emergency, the RCN Governance Support team will act on behalf of The Foundation, and liaise with the IT team to restore data in a timely manner.

8.3.2 RCNi has significant requirements for services that are provided by RCN Cardiff Gate. Should an incident affect Cardiff Gate, the Service Level Agreement between these two organisations sets out information on the services that will require re-instatement, and their priority.

8.4 Communications.

Experience has taught the organisation the value of clear, concise information paths during and immediately following an incident. All local Action Plans must clearly indicate who has responsibility for notifying and liaising with the Communications department, when contact should be initiated and how communications should be managed.

8.4.1 Appropriate media and content for communications.

The following subsections list the individuals and teams responsible for the content of any communications: however, the Communications Department will take responsibility for selecting and providing the appropriate media channels for those messages.

Staff must endeavour to avoid the use of unofficial, informal local communications as this may lead to the spread of rumour and hearsay at a time when clear, consistent, and unambiguous and messages are critical.

Likewise, the organisation recognises the impact that poor communication may have on its reputation - especially if message contents are beyond our control e.g. broadcast media, social networks. Consequently, Senior Managers must take particular care when communicating outside of the organisation.

8.4.2 Communicating to staff

Human Resources will take responsibility for communications related to the workforce and their work environment e.g. communicating decisions to open/close offices, communicating Health & Safety information, communicating information regarding office relocations.

Once the Executive Team has declared an emergency, it is essential that staff are kept up to date with progress and any decisions that may affect them and their work.

Faced with an emergency however, it cannot be assumed that emails or intranet will be available. An external website has therefore been created to give staff real-time information and guidance on topics such as using RCN computer systems, accessing offices, and any recommended work arrangements during the emergency.

Staff have received a card giving details of a website and telephone number, which will provide information and guidance in the event of local crises, national emergencies, or severe weather conditions. Responsibility for updating the contents of the website/telephone lies with the Communications team, and all requests to add content must be passed to them for approval and action.

8.4.3 Communicating to members.

The Business Recovery Team will ensure processes are in place to inform Council, Committees, Activists, and Members of any Business Continuity / Disaster Recovery issues - also ensuring they are informed of any alternative measures being put in place to support their continued working (e.g. alternative office locations, alternative IT infrastructures).

8.4.4 Communicating with Government, Department of Health, and similar.

In the event that the emergency results from a pandemic of similar health-related issue, the Royal College may be called on to offer timely and accurate clinical information and advice to enable healthcare professionals to treat patients appropriately. In such circumstances the information, and the means of communicating it, will be negotiated between the Government body, the Communications department, and the relevant RCN department/region.

8.4.5 Communicating with Broadcast Media and the Public.

All communications with Television, Radio or other Broadcast media will be managed by the media team of the Communications department. Local/regional Communications Managers will liaise with the External Affairs team when such communications are dealt with at a local/regional level.

In the event of a Cyber-attack on the RCN advice will be sought from the RCN Cyber Insurance providers to ascertain the messages to be communicated, this will be coordinated by the Head of IT or IT Operations Manager, who will work closely with the media team.

8.4.6 Financial communications between RCN and Insurers.

Following an incident, it is the responsibility of the Head of Finance (or their appointed deputy) to contact relevant Insurance Companies, and to notify them of the scope and scale of the incident. The Head of Finance will then act as the single point of contact between the Insurance companies and the RCN.

8.4.7 Cyber-attack communications between RCN and Insurers.

In the event of a Cyber-attack on the RCN advice will be sought from the RCN Cyber Insurance providers to seek assistance in dealing with RCN system restoration, this will be coordinated by the Head of IT or IT Operations Manager.

9. Testing and reviewing Business Continuity.

The Governance Planning Manager has responsibility for maintaining a process and schedule for the maintenance of business continuity documents and systems.

9.1 Post-incident reviews and logs for each incident.

Once an incident has been resolved, and business has stabilised, the organisation must take the time to review the background to the emergency, the actions that were taken, and the lessons that have been learned.

An online database exists to ensure such information is captured in a consistent manner, and is stored centrally as online electronic forms that can be used for incident analysis. Guidance is provided on holding post-incident reviews, and the information to be recorded within the database.

Cyber Security Incidents involving data categorised as “high confidentiality” or “sensitive data” will be so identified in order to implement the relevant regulatory compliance procedures, if necessary.

9.2 Document reviews.

All BCP documentation (both corporate and local) is to be reviewed and signed-off by the responsible manager(s) at least annually: the reviews should identify changes to personnel, office sites or systems.

All reviews must include a Business Impact Assessment (BIA), which will identify and assess critical IT requirements associated with the plan.

Reviews should involve all departments affected by a plan, and should also consider implications for the annual budget and planning calendar taking place simultaneously.

Action plans should then be updated and re-issued as appropriate. See Figure 3 for details.

Individual BCP documents are under the ownership and control of the responsible managers; however, those managers must inform the Governance Planning Manager of any updates.

The Governance Planning Manager is responsible for;

- Uploading copies of revised Action Plans to the emergency website for use by the Executive Team and Business Recovery Team[2].

- Maintaining a schedule that records the dates of Action Plan updates or reviews - ensuring version control and compliance with the annual cycle.

9.3 Testing BCP systems and processes.

The Governance Planning Manager will coordinate an annual test programme of all BCP action plans.

The programme will address the appropriate scope and scale of formal tests required to assure the organisation of its BCP capabilities. Three levels should be considered when developing the programme: (i) proving the backup and restoration of critical data and IT services (ii) simulated testing of Actions Plans and (iii) full testing of the Action Plans.

The programme will be developed in collaboration with IT, Health & Safety and Estates teams. Its scope and scale will take in to consideration any historic BCP events (including those captured in the BCP incident log), to identify any scenarios where the organisation already has/has not proven experience.

If appropriate, a small number of these exercises will be scheduled at the same time, allowing a multi-site/multi-department scenario to be tested.
Every Country, region, and department will take account of the lessons learned from their test when reviewing and updating their local Action Plan.

The Governance Planning Manager has responsibility for maintaining a schedule recording the dates of BCP tests, the outcomes and lessons learned.

--- End ---

[2] www.support.rcn.org.uk