



# **Lincolnshire Police Authority**

## **Business Continuity Scrutiny**

Report for the Audit, Risk and Governance  
Committee

November 2009

**Howard Hunt**  
Deputy Chief Executive

<b>1.0</b>	<b>Introduction</b> .....	Pages 4 - 6
	Purpose and Objective	
	Rationale	
	Scope	
	Exclusions	
	Panel Membership	
<b>2.0</b>	<b>Background</b> .....	Pages 7 - 9
	Definitions	
	Civil Contingencies Act 2004	
	ACPO/NPIA Guidance on Emergency Procedures 2009	
	Literature Review	
	Methodology	
	National issues	
	Local issues and the current situation	
	Lincolnshire Police Authority	
	Business continuity planning – key elements	
	Service levels	
	Risk analysis	
	Emergency/crisis action planning	
	Business recovery planning	
	Note on Terminology	
<b>3.0</b>	<b>Management and planning arrangements</b> .....	Pages 10 - 18
	Allocation of responsibilities and leadership	
	Governance and the new BC policy	
	Risk Management	
	Planning	
	Disaster recovery	
<b>4.0</b>	<b>Staff awareness and training</b> .....	Pages 19 - 20
	Culture	
	Understanding the importance	
	Awareness	
	Corporacy	
<b>5.0</b>	<b>Maintenance and testing</b> .....	Page 21
<b>6.0</b>	<b>Resourcing</b> .....	Page 22
	People	
	Capital Programme	
<b>7.0</b>	<b>Best practice and collaboration</b> .....	Page 23
<b>8.0</b>	<b>Challenges</b> .....	Pages 24 - 25
<b>9.0</b>	<b>Risks</b> .....	Pages 26 - 27
<b>10.0</b>	<b>Business Continuity requirements of the Police Authority</b> .....	Page 28
<b>11.0</b>	<b>Next Steps</b> .....	Page 29

<b>12.0 Recommendations.....</b>	<b>Pages 30 - 32</b>
<b>13.0 Appendices.....</b>	<b>Pages 33 - 58</b>

## 1.0 Introduction

### 1.1 Purpose and objective

The purpose of scrutiny is to contribute to the achievement and maintenance of high levels of performance, efficiency and effectiveness of the Force and Authority. Specifically this scrutiny aims to understand the Business Continuity Management (BCM) and Planning processes the Force has in place and identify where improvements can be made to increase the ability of the Force to maintain critical operational activities when these face disruption.

### 1.2 Rationale

The rationale for selecting the topic of Business Continuity (BC) is as follows:

- **Performance:** Business continuity planning increases the ability of an organisation to maintain critical operational activities when they face disruption and recover activities which may have ceased. Business continuity management processes and procedures therefore directly impact on an organisation's performance. A new Business Continuity Management policy is currently being developed by the Force. This scrutiny therefore has the opportunity to inform the policy's further development and implementation.
- **Risks:** Not having a business continuity plan (BCP) or keeping it up to date and tested would be contrary to the requirements of the Civil Contingencies Act 2004. Without appropriate BCM arrangements, the Force would not be prepared if operational activity was adversely impacted, resulting in longer recovery times, reputational damage and increased costs. The lack of preparedness could mean areas of poor resilience are not identified and the opportunity to mitigate risk lost. A particular area to consider and build on a previous scrutiny will be the Business Continuity arrangements for the Force Communications and Control Centre (FCCC). FCCC has previously suffered from power outage (Autumn 2008), adversely impacting on operations. Business continuity issues feature in the Force risk register.
- **Resources:** It is difficult to estimate exact costs given the cross cutting nature of the topic. The Force's objective analysis data places business continuity planning under the heading of civil contingencies that also includes contingency planning, purpose built command suites used during major/large incidents, emergencies or exercises and incident information centres. Under this heading the Force has allocated two Constables (special events and licensing) and two support staff (emergency planning officer and assistant), with a cumulative total annual cost of £143,623. There are senior staffing costs and other costs that are not reflected in this figure.
- **Impact on local communities:** The impact of this scrutiny topic is particularly significant to the communities of Lincolnshire, as it is focused on the ability of the Force to maintain a police service throughout the County if operational activity were to be adversely impacted. In such an event it would therefore link to the general public's overall perception and feelings of trust, confidence and satisfaction of policing services.

- **National Policy:** As detailed above, the Force has a statutory obligation under the Civil Contingencies Act 2004 to maintain a business continuity plan. The Association of Chief Police Officers (ACPO) and the National Policing Improvement Agency (NPIA) also recognise the need for increased resilience in police forces to be able to continue to provide critical services during an incident that could impact on a Force's own business processes.
- **Inspections:** Business Continuity forms part of the Protective Service Inspection of Civil Contingencies and Emergency Planning. This took place last year. Lincolnshire was not inspected during this phase of inspection due to the County being classified as a low risk area. The ACPO Business Continuity working group has worked closely with Her Majesty's Inspectorate of Constabulary (HMIC) to ensure that forces' business continuity plans are part of a measurable audit process. The role of the HMIC is to promote efficiency and effectiveness of police forces and, as such, ACPO's view is that business continuity plans should be measured to meet the public expectation that police forces will continue to protect them, even in catastrophic circumstances.
- The topic of Business Continuity is considered to be **cross-cutting** as it has implications for all divisions and departments across the Force.
- **Priorities/adding value:** The Panel and Force agree that the scrutiny will **add value** and build on planned activities within the Force; particularly the development of the new policy and the following commitments in the Policing Plan and for Lincolnshire 2009-2012.:

"In 2010/11 we will:

Ensure procedures are in place regarding our essential support activities to mitigate risks from disaster (disaster recovery and business continuity)

In 2011/12 we will:

Implement new structures and processes, to ensure that we can continue to provide a comprehensive policing service to you, if there is a technical or business failure."

- The scrutiny will not **duplicate** any work being conducted by the Force and it is hoped it will inform the achievement of these two objectives.
- The scrutiny is considered to be **timely** and **ethical** and it can be effectively **resourced**.

### 1.3 **Scope**

In order to maximise the benefits from the scrutiny process, the Panel plan to explore the following specific areas relating to Business Continuity:

- The Force's current and in-development business continuity management processes including planning, governance, risk management, business/disaster recovery strategy and allocation of responsibilities.
- The Force's arrangements for staff awareness and training.
- The Force's arrangements for maintaining, reviewing and updating business continuity plans and their testing.
- Identify best practice (other Forces, NPIA, ACPO, British Standards Institute).

- Consider opportunities for collaboration, both regionally with other Police Forces and locally with Local Area Agreement (LAA) partners and the formalisation of these through agreed protocols.
- Consider the Business Continuity Planning requirements of the Authority given the Authority's dependency on the Force for key services (e.g. ICT, telephony) and accommodation.

1.4 In carrying out the above the Panel will particularly wish to consider whether critical business areas have been appropriately identified, risks and threats adequately assessed, that disaster recovery/contingency planning is sufficient and what guidance can be offered to the Force to aid planning in these areas. Priority areas suggested by the Force include FCCC, the Force estate, ICT and workforce contingencies in the event of large scale absence including chief officers.

1.5 All of the above is to be done with reference to the statutory obligations under the Civil Contingencies Act 2004 and best practice as identified by the British Standard on Business Continuity Management BS25999 and the ACPO/NPIA Guidance on Emergency Procedures.

## 1.6 Exclusions

To ensure that the scrutiny remains focussed and deliverable within time and resource constraints, the Panel will not be able to consider all aspects of Business Continuity and contingent/interrelated areas.

The following exclusions will apply:

- An active test of the Force's Business Continuity Plan
- Planning related to Force operational response to emergencies or major incidents regardless of their cause.

Significant work is being undertaken by Nancie Shackleton the Head of Strategic Development around contingency planning for the potential effects of swine flu. The Panel understand this work is well advanced. This should not be excluded from the scrutiny, but it maybe that there are other areas where the Panel could add greater value and so will prioritise their work and its depth accordingly.

## 1.7 Panel Membership

The scrutiny Panel comprised the following members:

Mrs Angela Crowe JP - Audit, Risk and Governance Committee - Panel lead  
 Mr Paul Przyszlak – Audit, Risk and Governance Committee  
 Mr John Atter – Audit, Risk and Governance Committee

The Panel were supported in their work by the following Authority officers:  
 Howard Hunt – Deputy Chief Executive  
 Ginny Mason - Research and Performance Officer

## **2.0 Background**

### **2.1 Definitions**

The British Standard on Business Continuity Management (BCM), BS25999, defines BCM as “a holistic management process that identifies potential threats to an organisation and the impacts to operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.”

2.2 A Business Continuity Plan (BCP) identifies the impact of potential threats and formulates viable strategies which ensure continuity and/or recovery of an organisation’s operational activities.

2.3 Cabinet Office UK Resilience guidance states that BCM “Must be regarded as an integral part of an organisation’s normal ongoing management process.”

### **2.4 Civil Contingencies Act**

The Civil Contingencies Act 2004 requires Category 1 responders, which include Police Forces, to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable.

The BCM duty in the Act relates to all the functions of a Category 1 responder, not just its civil protection functions. Hence the legislation requires Category 1 responders to maintain plans to deal with emergencies and put in place arrangements to warn and inform the public in the event of an emergency. But it also requires them to make provision for ensuring that their ordinary functions can be continued to the extent required. The Regulations also require Category 1 responders to put in place a training programme for those directly involved in the execution of the BCP should it be invoked.

### **2.5 ACPO/NPIA Guidance on Emergency Procedures 2009**

This national guidance recognises the importance of business continuity management and the statutory obligations placed on Police Forces. (Appendix 3)

### **2.6 Literature review**

In addition to the legislation and guidance referred to above, the Panel has also reviewed other source documents. The Panel has reviewed all current and expired business continuity plans in existence across the Force together with the relevant new and existing policies. Key documents reviewed are listed at Appendix 3.

### **2.7 Methodology**

In addition to literature review, the Panel interviewed Force officers and staff during August and September 2009. The Panel is grateful for the participation of all those interviewed. They particularly wish to acknowledge interviewees’ openness and honesty in answering questions and sharing knowledge which contributed greatly to the Panel’s learning of the issues and the conclusions drawn in this report. A full list of those Force officers and staff interviewed by the Panel can be found at Appendix 6.

## 2.8 **National issues**

Mike Bowron, Commissioner of the City of London Police, is the National ACPO champion for business continuity and chairs the ACPO business continuity working group. Additionally, Mr Meredydd Hughes, Chief Constable South Yorkshire, is the national lead on Emergency Procedures which includes the elements of business continuity related to emergency planning.

## 2.9 **Local issues and the current situation**

The Panel were pleased to note that the Force openly recognises that business continuity and recovery arrangements within the organisation require development. From the Panel's work it is clear this recognition exists to varying degrees across the Force and this was acknowledged by the Deputy Chief Constable who is the Chief Officer lead in this area. The Panel also recognise that a number of business continuity and disaster recovery issues are reflected in the Force risk register. Building on the Authority's previous scrutiny into the FCCC, the Panel shares the Deputy Chief Constable's view that both the FCCC and ICT services across the Force are key risk areas. These areas are addressed in detail within the report. It is accepted by the Panel that local gaps in business continuity planning are not unique to Lincolnshire however, given the Force's planned development in BCM, the Panel is of the view that Lincolnshire could become an exemplar for others to follow.

2.10 The Panel is mindful that this scrutiny is being conducted at a time when considerable development work is underway in the form of a new policy and the introduction of a new approach to business continuity management within the Force. The Panel therefore sees the timing of this scrutiny as an opportunity to inform and add value to the policy's continuing development and its implementation, whilst also learning from existing arrangements.

2.11 The Panel recognises that business continuity management may not naturally be in the culture of police forces as the focus of their activities is often required to be on successful immediate crisis management. Recognising the strengths that Lincolnshire has in this field, the Panel believes effective business continuity management will help the Force to react appropriately to an event or multiple events and also recover. Rather than being a constraint, robust BCM informs proactivity and can ensure an organisation is in the right place at the right time and better placed to deal with more complex scenarios and risks.

## 2.12 **Lincolnshire Police Authority**

The Authority does not have any formal Business Continuity arrangements of its own. In carrying out this scrutiny it is recognised both that this needs to be addressed and that, as the Authority is reliant on the Force for provision of key services and infrastructure essential to the delivery of its business, any planning needs to be carried out in close co-operation with the Force.

## 2.13 **Business continuity planning – key elements**

In conducting this scrutiny the Panel is mindful of the following key elements which represent good practice in business continuity management.

- 2.14 **Service Levels:** An organisation must understand its *desired* level of service and its *minimum* acceptable level of service. A business continuity plan outlines how to get from the minimum service level to the desired service level in the shortest possible time.
- 2.15 **Risk analysis:** Risks that face an organisation should be mapped and the consequence of these risks occurring must be understood (through business impact analysis). Protection and mitigation measures must then be put in place to ensure that an organisation will always be able to provide its minimum level of service, whatever happens.
- 2.16 **Emergency/crisis action planning:** This should deal with the immediate aftermath of any incident and enables the business to maintain the minimum service level across all of its business spectrum following an incident.
- 2.17 **Business recovery planning:** This should deal with the return to normality and desired service levels.
- 2.18 **Note on terminology**  
This report is keen to make the distinction throughout between business continuity and business or disaster recovery and the importance of both aspects. However it should be assumed that where the text refers only to Business Continuity Plans (BCPs), this includes both phases, i.e. continuity and recovery planning as the Panel would envisage these would be covered in a single BCP document.

### **3.0 Management and planning arrangements**

3.1 As part of the scrutiny Panel's exploration of the Force's current and in-development business continuity management processes Panel members reviewed planning, governance, risk management, business/disaster recovery strategies and allocation of responsibilities.

#### **3.2 Allocation of responsibilities and leadership**

The Deputy Chief Constable (DCC) is the chief officer lead for business continuity. He acknowledged that prior to his taking up post there was no chief officer lead for BC. The Panel were pleased to note the DCC's enthusiasm for driving forward the work in progress and that he will chair the Business Continuity Management Board proposed in the new Force policy (see below).

3.3 In its interviews with officers and staff the Panel encountered a range of perceptions as to whether business continuity management was being "driven" by the Chief Officers Group. The Panel recognises that until the new policy has been formally approved differing perceptions may persist. However a key recommendation of the Panel is that once work to implement and embed the new business continuity management approach outlined in the new policy commences, it should be evident to all in the organisation that there is a strong lead and consistent corporate approach to BCM across the Force.

**Recommendation 1: It is recommended that the Force embeds a corporate, consistent and centrally led approach to BCM throughout the Force.**

3.4 Ian Watkins, Emergency Planning Officer, has drafted the new Force business continuity policy. Ian reports to the Head of Operations Support, which sits within the Assistant Chief Constable (Protective Services) portfolio. As Emergency Planning Officer Ian's responsibilities include, but are not limited to, business continuity.

3.5 Nancie Shackleton, Head of Strategic Development, is strategic lead for business continuity, disaster recovery and risk management. She has also acted as lead on provision of command support to the Crisis Management Team formed to address swine flu contingency planning within the Force. She reports directly to the Deputy Chief Constable.

3.6 Ian Watkins currently sits within the Operations Support Department. During the course of this scrutiny the Panel became aware that consideration was being given to his role becoming part of Strategic Development within the DCC's portfolio. The panel supports such a move as this will help embed a more joined-up approach to BCM and centralise key responsibilities.

**Recommendation 2: It is recommended that the Emergency Planning Officer be located in Strategic Development.**

3.7 Nicky Prutton, programme and planning manager, reports to Nancie Shackleton. Risk management is part of Nicky's portfolio and she also manages Ian Rushton, project manager for Disaster Recovery. Ian is delivering a project focussing on the FCCC and ICT server capability. The

Panel were informed that this project is currently at “scoping” stage and it is considered in more detail later in this report.

- 3.8 In relation to leadership, it was clear from the Panel’s interviews that there was lack of clarity for many about what the Force expected of them in terms of BCM. Recommendation 1 goes some way to addressing this however, the Panel makes a number of additional recommendations on this subject and these are covered in the section headed Staff Awareness and Training.
- 3.9 It is also the Panel’s observation that a perceived lack of leadership on BCM in the past has resulted in the development of BC plans taking place in isolation within divisions and departments. This particular issue is also addressed in more detail later in the report in the planning section, including the inherent risks in such a strategy, but it is highlighted here as something that can be addressed through the effective leadership the Panel recognises the DCC is keen to provide.

### 3.10 Governance and the new BC policy

As mentioned above, Ian Watkins has drafted a new Business Continuity Policy which outlines a number of objectives. The full policy is attached at appendix 5. It is his view that good application of the policy will result in BCM processes that reflect the good practice described in BS25999. This would also lead the Force to be regarded as complying with the BC requirements laid down in the Civil Contingencies Act (CCA) 2004. Thirdly the Force would have BCM processes which deliver resilience to most risks and the ability to adjust working practices and service delivery to maintain reasonable levels of service in all reasonably anticipated circumstances. These are all aspirations which the Panel believes the Force should plan to achieve. In so doing it has to be recognised that current arrangements neither represent effective BCM nor demonstrate compliance with the CCA.

- 3.11 Whilst recognising the new policy was in development, during their interviewing, the Panel has received conflicting messages about its progress. Their broad understanding is that the policy has now been approved in principle by Command Group and is entering consultation across the Force. Final approval and implementation is therefore anticipated within eight weeks (by December 2009). The DCC suggested full implementation of the policy would take 5 years and that the Force would address the critical risk areas in the first year and then others.
- 3.12 The Panel broadly supports the objectives in the policy but believes further work needs to be undertaken to specify the work required to meet its objectives. The Panel recommends that once the policy is formally approved a project management approach be adopted to plan, prioritise, monitor, manage and evaluate the activity which will deliver the policy’s objectives. Clear timelines with measurable outcomes need to be set for this work. It is the Panel’s recommendation that this be done as soon as is reasonably practicable.

**Recommendation 3: It is recommended that following formal approval of the new BC policy, the Force adopt a project management approach to managing the work necessary to deliver the project’s objectives.**

- 3.13 A key concept within the new policy is the creation of a *Business Continuity Management Board* to be chaired by the Deputy Chief Constable.
- 3.14 The panel supports the formation of such a group as a mechanism for managing the implementation of business continuity arrangements within the Force, as well as providing governance and a strategic framework. It recommends the Board have clear terms of reference and that it be in place as soon as practicable to oversee the policy's implementation once formal approval has been obtained.

**Recommendation 4: It is recommended the Force forms a business continuity management board to oversee the implementation of BC arrangements within the Force.**

- 3.15 It was recognised by many interviewees and the Panel concurs that there is a risk that a policy can become a static document which "sits on a shelf". The Panel therefore see the DCC's leadership and the role of the BC Management Board as crucial in both driving forward the necessary project work needed to ensure robust BCM, but also in monitoring, reviewing and maintaining effective BCM in perpetuity.

**3.16 Risk Management**

At the time of writing risks relating to the loss of mains power supplies to ICT services, generic disaster recovery and specific ICT disaster recovery feature in the Force risk register, with these risks owned by the Head of ICT, the DCC and Head of ICT respectively.

- 3.17 The lack of effective or non-existent disaster recovery and business continuity plans which could result in a disruption or failure of business within the Force is also identified as a risk within the register. This risk is owned by the DCC.
- 3.18 The risks to the continued operation of the FCCC, largely underpinned by ICT services, are owned by the Head of ICT.
- 3.19 The potential loss of the main servers at Headquarters which service the entire Force network are an additional risk owned by the Head of ICT. Lack of testing of plans to cope with loss of computer systems is also highlighted as a risk.
- 3.20 The Panel is pleased to acknowledge that the DCC recognises all of the above areas as major risks and that controls proportionate to the risks identified are urgently required. Many of those interviewed concurred. The Panel agrees that the areas do represent the key risks.
- 3.21 Risk management within the Force is overseen by a risk management board which is chaired by the DCC. The board reviews organisational risks, assigns risk owners and monitors organisational risks to the Force.
- 3.22 As risks and their management represent an intrinsic part of BCM, issues relating to the subject arise throughout the report. However in a later section the Panel takes the opportunity to address some specific points, but at this point it is recommended that the Force assures itself that the oversight,

ownership and management of these risks by the risk management board are properly aligned with the role of the proposed Business Continuity Management Board to ensure clarity and eliminate duplication.

**Recommendation 5: It is recommended that the Force assures itself that the oversight, ownership and management of risks relating to BC which appear on the Force risk register are properly aligned with the role of the proposed Business Continuity Management Board to ensure clarity and eliminate duplication.**

### 3.23 Planning

- 3.24 As noted in the introduction, the Panel reviewed all existing business continuity plans across the Force. It was pleased to find that most divisions and departments had some form of BCP. However, the quality of these and therefore their likely robustness if instigated was found to be variable. The Panel believes a number of factors have contributed to this situation. Issues of leadership have been addressed earlier in this report and it is clear that in the absence of a well enforced force-wide policy which outlines what is required, quality of planning will be adversely impacted. It is also evident that staff awareness and training can be much improved and these are addressed later in this report.
- 3.25 An additional area of concern for the panel was that these plans had, on the whole, been developed in isolation. There are a number of recommendations that stem from this “silo” approach.
- 3.26 Firstly, it is the Panel’s view that there are a number of generic risks that should be dealt with in overarching, force-wide BC plans. These should include at the very least loss of ICT, utilities, people and estate. These issues should always be dealt with centrally rather than independently within departments and divisions as it is very likely they will impact across divisional/departmental boundaries.

**Recommendation 6: It is recommended the Force introduces force-wide business continuity plans that address generic loss likely to impact the organisation as a whole e.g. ICT, utilities, people and estate in addition to divisional/departmental BCPs.**

- 3.27 It is the Panel’s view that the tendency for business continuity plans to be developed in isolation fails to consider the interdependencies between divisions and/or departments. The Panel believes there is inherent and necessary value in those who are closest to specialist operations taking responsibility for the detail of BCM in their area of work, but this must *inform and be informed by* a Force wide approach, particularly with regard to the prioritisation of continuity and recovery of critical functions. Prioritisation of critical functions has to be a top-down process to ensure consistency and inform effective Force-wide business continuity and recovery.
- 3.28 Even before prioritisation can be carried out, a foundation of business continuity management is the detailed analysis of an organisation’s activities and the determination of the minimum acceptable and preferred levels of service for critical functions. The Panel is not aware this has been carried out. Nor have detailed business impact assessments taken place identifying the risks the Force’s activities face, the likelihood of them being disrupted and the resultant consequences.
- 3.29 As part of the swine flu contingency planning work, the Panel understands that Force functions were classified into three “tiers”. As mentioned previously, identifying and prioritising both the continuity and recovery requirements for critical functions are key requirements of effective BCM. The Panel understands that this work has yet to be completed, both in terms of the identification of all functions and their prioritisation. The Panel does however commend the work to date. It is now recommended that this work is

considered as part and parcel of business continuity management. Functions and their prioritisation will be the same whatever the threat to their continuity. Decisions on defining these must be taken at a senior level and embedded across the Force. The Panel also understands that the NPIA has issued national guidance around IT critical functions. This needs to be taken into account.

**Recommendation 7: It is recommended the Force a) maps and defines its critical functions, b) defines the desired and minimum acceptable levels of service for these functions, c) conducts business impact analyses to understand the risks to these functions, the likelihood of disruption occurring and the consequences and d) prioritises the continuity and recovery of these functions. This work should then inform both Force-wide and departmental/divisional BCPs. This approach should be clearly outlined in policy and co-ordinated and led by the BC Management Board.**

3.30 Whilst being informed by this methodology, it is the Panel's opinion that Business Continuity Plans for specific functions/departments/divisions must also be reviewed centrally to ensure they interlink where appropriately and do not conflict. The instigation of a particular business continuity plan within one department may result in other departments having to instigate their own plans if they are reliant on critical functions from elsewhere which are no longer being delivered.

**Recommendation 8: The Business Continuity Management Board review and approve departmental/divisional BCPs to ensure consistency with the above methodology outlined in recommendation 7 and that interdependencies between parts of the Force have been properly assessed and accounted for.**

3.31 The Panel felt it important to note that the DCC outlined to them his experience in Carlisle when a Divisional Headquarters was rendered inoperable by flooding. There was no business continuity plan in place and it was the DCC's view the Cumbria force was ill prepared as a result. He is therefore of the view that disasters do occur and need to be planned for. There was disruption within the Cumbria force for three years as a result of the flooding. The DCC therefore also recognises the importance of recovery planning within BCM.

3.32 Many of those interviewed by the Panel accepted that in the absence of detailed BCPs, much information which would be expected to be in a plan was held in individuals' heads. This emphasises not only the need for more detailed BC planning, but also that the absence of key individuals should be anticipated in BCPs. Key roles identified in BCPs should have named deputies who are fully cognisant with what would be required of them should the eventuality arise.

3.33 It was also apparent that the content of some plans was based on assumptions rather than facts. For instance if a plan identifies that a particular building maybe available from a third party as a temporary option to mitigate loss of Force estate, the availability and functionality of this should be secured and assessed at the time of writing the plan, rather than the plan being instigated only to discover the option isn't viable.

3.34 The need to plan robustly for business continuity and recovery becomes increasingly important when faced with high-impact or multiple risks to the

Force's key functions. The panel shares the opinion of many of those interviewed when it cites the FCCC and force-wide ICT provision as areas which deserve particular attention in this report. As mentioned elsewhere the Force has successfully solved problems spontaneously in the heat of a crisis without detailed plans. But the absence of detailed planning exposes the Force to the more complex risks found in ICT provision and the operation of the FCCC.

- 3.35 As noted above, Ian Rushton is currently managing a disaster recovery project which will consider the FCCC and the ICT servers. The Panel were told that this project was currently at "scoping stage" and this was to include exploring the possible parameters for disaster recovery, including an assessment of risk and likelihood of incident occurrence, with an associated cost profile which would, in turn, inform the Capital Programme.
- 3.36 The Panel were unclear of the timelines for this work. There was also a lack of clarity of how this work related to the Force's strategic approach to business continuity and the development of the new BC policy. This was seen as a particular concern given the risks associated with the FCCC and ICT server infrastructure. The Panel recommends that the BC management board gives a clear steer on the remit and timelines for this work as part of the Panel's recommended approach that the board project manage the work necessary to implement the new Force BC policy. It is also the Panel's opinion that any recommended mitigation requiring capital investment should be appropriately prioritised within the Capital Programme in the context of the impact and likelihood of failures in ICT provision or FCCC service.

**Recommendation 9: It is recommended that the ICT and FCCC disaster recovery projects be overseen by the Business Continuity Management Board, that a clear remit and timeline prioritise this work and that any mitigation requiring capital investment be appropriately prioritised within the Capital Programme.**

- 3.37 The Panel recognises that both ICT provision and the FCCC may often be reliant on support and back-up arrangements provided by third parties in the event of an incident. The Panel therefore recommends that the procurement process for business critical service contracts such as ICT support include an assessment of the contractors' own business continuity arrangements to ensure they would be able to continue to deliver the Force's requirements should an event impact on their own operational arrangements.

**Recommendation 10: It is recommended that the Force procurement process for business critical service contracts (such as ICT support) include an assessment of the contractors' own business continuity arrangements to enable the Force to satisfy itself that contractors would be able to deliver in the event of their own operations being compromised.**

- 3.38 It is widely recognised by the Force and the Panel that a critical area of the Force's operations is the FCCC. The Panel acknowledges the assistance provided in the past by Nottinghamshire Police when the ability of the FCCC to function has been compromised. The Panel has concerns however that given both the importance of the FCCC and the risks already in existence on a day to day basis, arrangements to seek support from neighbouring Forces may not be robust in a serious incident. It is the Panel's opinion that any

agreements with other Forces need to be formalised, both for the FCCC and other areas, but as a matter of priority for the FCCC. In so doing, these need to take account of whether secondary measures are necessary to mitigate the risk that if a neighbouring Force has also instigated their own business continuity plan that Force's priority would undoubtedly be the continuity of their own functions rather than assisting Lincolnshire with the continuity of theirs.

**Recommendation 11: It is recommended that the Force seek to formalise any agreements with other forces or agencies for the provision of mutual aid where this forms part of the Force's business continuity planning. Formalising these agreements should be prioritised in line with the business impact analysis referred to elsewhere in this report, i.e. focussing on the areas of greatest risk and impact first.**

3.39 The Panel also found it concerning that for some critical functions there were inconsistencies in the views of those they interviewed as to whether there were formal protocols in place with other Forces. This needs to be resolved in the Force's BCPs as misinformation and misunderstandings by individuals represent a serious risk to effective business continuity and recovery, particularly if the correct knowledge rests with an individual who is not present when a BCP is instigated.

**Recommendation 12: It is recommended that the Force ensure any formal protocols/agreements for mutual aid be properly documented in the relevant business continuity plans.**

3.40 The Panel returns to the subject of ICT and the FCCC in the "risk" section later in this report.

### 3.41 **Disaster recovery**

3.42 As noted earlier, a key element of BCM is disaster recovery, i.e. returning all of the critical functions back to the preferred level of delivery. The Panel felt this was a weakness both in the written plans currently in existence and in the answers given to the Panel's questions. Very few of the plans reviewed by the Panel covered this phase. Many interviewees accepted this was a weakness, a position the Panel endorses and believes requires action.

3.43 It is therefore recommended that Force BC Plans include robust strategies for disaster recovery and the return of operations to preferred service levels. Best practice is that this planning should cover the 90 days immediately following the incident that has led to the invocation of the plan. This process of recovery needs to be prioritised for all critical functions. This prioritisation can, in part, be informed by the use of the business impact analyses recommended earlier. However, it is important to note that priorities in the recovery phase may be different to those in the immediate aftermath of an incident. Top level plans should reflect this. Again, although the recovery phase planning should be informed by divisions' and departments' needs, it should be co-ordinated Force-wide to ensure consistency and that individual departmental priorities enable Force-wide priorities to be met. It is therefore recommended that the Business Continuity Management Board co-ordinates this work.

**Recommendation 13: It is recommended Force business continuity plans include recovery strategies for the first 90 days following an incident which aim to return functions to preferred service levels. This should be co-ordinated by the BC Management Board.**

## 4.0 Staff awareness and training

- 4.1 The Panel understand that the Emergency Planning Officer is the only formally trained business continuity resource in the Force. It was recognised by all those interviewed that training was not provided as standard to key staff in the Force and this needed to be addressed.
- 4.2 It should also be noted that the Civil Contingencies Act 2004 requires Category 1 responders to put in place a training programme for those directly involved in the execution of their BCPs.
- 4.3 It is the Panel's view that a chief officer, probably the DCC given he is the lead for BC, receives formal training on business continuity. The Panel also believe training and general awareness raising is necessary not only to implement the new BC policy and resultant plans, but also to embed BCM within the Force. The Panel believes there are a number of issues that need to be addressed within this.
- 4.4 **Culture:** As mentioned elsewhere in this report, it is evident that the mindset within the Force when considering BCM is heavily focussed on crisis management. It is recognised that crisis management is a strength within the Force and that its capabilities in this area contribute to the ability to manage Force activities on a day to day basis. The Force often successfully tackles crises without formal plans having been drawn up in advance. The Panel acknowledges that in operational policing matters this approach is both accepted and effective. Every eventuality cannot be planned for and it is one of the Force's great strengths that it can tackle unpredicted serious incidents "on the hoof." However the main (i.e. generic) issues likely to be faced in a business continuity crisis scenario can, on the whole, be anticipated and therefore planned for, allowing for a measured and systematic response. Planning in the Panel's view does not restrict scope for the Force to utilise its undoubted crisis management skills, rather it enhances the effectiveness of them.
- 4.5 Whilst it is recognised that cultural shifts take time, it is the Panel's belief that general awareness raising and training, together with clear steers through the management and leadership chain, will enable the Force to become more comfortable with the elements of BCM and see its benefits.
- 4.6 **Understanding and importance:** The Panel were concerned that some of those interviewed were dismissive of the importance of BCM. It is unclear whether this is due to the crisis management culture, a general lack of understanding of what BCM is and therefore a fear of the unknown or, more worryingly, that individuals do not see it as their responsibility. It is the Panel's view that BCM is a key element of every management and leadership role within the Force and therefore should be reflected in relevant job descriptions.

**Recommendation 14: It is recommended that BCM responsibilities be reflected in relevant job descriptions of police officers and staff in management and leadership roles.**

- 4.7 **Awareness:** In addition to BCM being part of the management role, the Panel is of the view that all staff should have a basic understanding of what BCM is,

and what their role would be in the event of a BCP being implemented. The Panel's opinion is that current awareness across the Force was below an adequate level for effective plan implementation.

- 4.8 **Corporacy:** As mentioned elsewhere, for the Force's BCM arrangements to be robust and embedded across the organisation, the process should be led from the top and co-ordinated centrally. A silo approach to BCM is unlikely to work in the event of an incident which impacts across more than one business area. Any general awareness raising and training should deliver a clear message that BCM is a force-wide issue.

**Recommendation 15: It is recommended that the Force develop and implement a Force-wide Business Continuity training and awareness raising strategy, overseen by the Business Continuity Management Board.**

## **5.0 Maintenance and testing**

- 5.1 The Force does not currently have a Force-wide policy in place to cover maintenance and testing of existing BC plans. The Panel believes this is required.
- 5.2 Testing business continuity plans was on the whole seen as a risk by many of those the panel interviewed. The panel accepts that full live tests which require the suspension of critical functions may not be appropriate where robust back-up arrangements are not in place e.g. the FCCC. It is the Panel's experience however that live testing can be carried out in such a way that elements of a plan can be tested without undue risk to the continuity of critical functions. They are also of the view that table-top testing, properly facilitated and managed, can be a valuable tool in testing the robustness of plans and offers a learning opportunity for individuals in a risk free environment.
- 5.3 The Panel believes it also essential that BCPs are maintained regularly to reflect changes in functions, priorities and staff. It is recommended that a plan refresh take place whenever officers or staff who have responsibilities in a plan leave the Force or move to a different role. In addition a more formal review of each BCP should take place on an annual basis to ensure functions and prioritisation are up to date in the light of any operational changes.

**Recommendation 16: It is recommended that the Force develop co-ordinated testing and maintenance strategies for business continuity plans, monitored by the Business Continuity Management Board. Testing should comprise live and table-top testing proportionate to the criticality of the functions individual plans cater for.**

## **6.0 Resourcing**

### **6.1 People**

There was a general feeling emanating from those interviewed, which the Panel shares, that given the Force's ambitious plans for BCM, current personnel resources are inadequate.

6.2 The Panel recognises the enthusiasm, commitment and knowledge Ian Watkins has for BCM and the size of the challenge he is tackling in developing the Force's resilience in this area. It was observed by many of those the Panel interviewed and is the Panel's own opinion that despite Ian's undoubted commitment, the amount of resource he is able to devote to BCM at a critical phase in its development is not sufficient for the task facing the Force. Whilst acknowledging the work currently also being undertaken by Ian Rushton and that the issue of resourcing is being considered by Command Group, the panel recommends the Force considers its longer term resource needs to enable effective implementation of the new policy's objectives.

6.3 It should be noted however that once much of the implementation work has been completed, the personnel resource requirement will diminish significantly as on-going maintenance of BCM should largely be shared across the Force.

**Recommendation 17: It is recommended the Force gives due consideration to the long term personnel resources required to deliver the objectives it is setting itself for BCM and the appropriateness of current arrangements.**

### **6.4 Capital programme**

The Panel accepts that risk management and mitigation have to be carried out with due regard to financial matters including value for money. The Panel does not however share the view expressed by some of those interviewed that financial constraints act as an insurmountable barrier to appropriate and considered controls being put in place.

6.5 The Panel accepts and believes it necessary that capital expenditure will be required to ensure the FCCC has a robust back-up facility and for the continuity of force-wide ICT provision to become more resilient. It is not for the Panel to determine the detail of this or approve capital works. However the Panel recommends that the Force consider expediting the disaster recovery projects for the FCCC and ICT provision and that resultant recommendations requiring capital outlay be accurately factored into the capital programme and prioritised appropriately. Whilst the Force risk register indicates capital has been put aside to increase resilience in these areas, any existing needs identified in the capital programme will clearly require review once the disaster recovery projects have identified and recommended risk mitigation actions.

**Recommendation 18: It is recommended the Force consider expediting the disaster recovery project for the FCCC and ICT provision and that resultant recommendations requiring capital outlay be accurately factored into the capital programme and prioritised appropriately following further consultation with the Authority.**

## **7.0 Best practice and collaboration**

- 7.1 It has been noted elsewhere in this report that the Force has in place various agreements with neighbouring forces for them to offer assistance in the event of the inability of Lincolnshire to deliver its critical functions and the Panel has recommended these agreements be formalised earlier in this report.
- 7.2 The Panel understands that the remit of the East Midlands Collaboration Board does not currently include business continuity. It is the Panel's view that there is potential value to be gained from exploring opportunities for collaboration with partners, not only the East Midlands and other neighbouring police forces but also with the county and district councils, the Fire and Rescue Service, the probation service and the Crown Prosecution Service. These partnerships may offer options around pooling knowledge and sharing training as well as assistance when a BC plan is implemented. However such work would need to be appropriately prioritised alongside other developments with the Panel taking the view that embedding robust BCM internally, together with the formalising of protocols for assistance in the delivery of key functions such as the FCCC with other police services, are of greater urgency.
- 7.3 It is however recommended that the Force continues to attend the regional business continuity forum as an opportunity to share best practice and begin exploring wider collaboration possibilities.

**Recommendation 19: It is recommended that the Force continues to attend the regional business continuity forum and that they give thought to wider opportunities for collaboration once BCM internally is more robust.**

## 8.0 Challenges

- 8.1 The major challenges facing the Force have been well documented throughout this report, but the panel takes this opportunity to emphasise those which it sees as fundamental to the successful implementation of effective BCM arrangements.
- 8.2 In the Panel's opinion one of the major challenges with regard to embedding effective business continuity practices is that of culture. This is closely interlinked with the need for an increased understanding across the Force of what robust business continuity planning looks like.
- 8.3 The Panel believes that for the Force to meet its BCM objectives, there needs to be a coordinated and consistent effort across the organisation to emphasise the importance of BCM, in particular underlining that it is not simply crisis management. This can only be achieved through the delivery of effective communication and strong leadership, together with a formalised approach to determining required levels of staff awareness and knowledge, followed by the implementation of a strategy to achieve these.
- 8.4 It is the Panel's opinion that all managers must see BCM as part of their management role and it should therefore be reflected in relevant job descriptions.
- 8.5 Maintaining business continuity management as a current and on-going issue represents a challenge for all organisations. Plans must be continually reviewed, maintained and tested. BCM is a constant, not a discrete project that once completed can be filed away.
- 8.6 The issue of embedding a joined up approach to BCM across the Force needs to be addressed. The tendency for business continuity plans to be developed in isolation without any consideration of the interdependencies between parts of the organisation needs to change. It is the Panel's opinion that there is inherent value in those who are closest to specialist operations taking responsibility for the detail of BCM in their area of work, but this must inform and be informed by a Force wide approach, particularly with regard to the prioritisation of continuity and recovery of critical functions.
- 8.7 The Panel recognises that in the development of a new BCM policy the Force has begun the work that is required. The key now is to deliver on the policy's objectives.
- 8.8 A view was expressed by some interviewed that their perception was that the Force was not appropriately prepared to deal with the business continuity aspects resulting from the Force having to deal with a major operational emergency or incident. It was not in the Panel's remit to actively consider the impact of large scale operational activities on generic business continuity. The Panel is also mindful that perceptions are also not necessarily representative of the reality. The Panel would however recommend that the Force look at whether their generic business continuity planning would cover the eventuality of large scale abstractions (e.g. as anticipated for London Olympics 2012) or large scale resource redeployment of officers and staff on a large scale high-profile incident such as those recently experienced by other Forces.

**Recommendation 20: It is recommended that the Force considers whether its generic business continuity planning offers sufficient robustness to deal with large scale redeployment or abstractions to either major incidents within Lincolnshire or to other Forces.**

- 8.8 Finally, obtaining clarity of force-wide critical functions and the priorities for their continuity and recovery naturally leads to potentially conflicting views and some difficult choices. This is why the Panel has recommended business impact analysis and co-ordination by the Business Continuity Management Board. The panel sees its recommendations in the planning section of this report as vital in assisting the Force.

## 9.0 Risks

- 9.1 It is the Panel's view that the Deputy Chief Constable has a good understanding and recognition of the major risks with regard to Business Continuity. The Panel also believes that the description of risks as captured within the Force risk register is appropriate (*see risk management, para 3.16*).
- 9.2 Risks facing the Force have been well documented throughout this scrutiny, but the Panel felt it would be helpful to specifically address the most significant risks as articulated in the risk register.
- 9.3 In terms of the lack of effective or non-existent disaster recovery and business continuity plans the Panel is assured that progress is being made in this area, subject to the Force's response to the recommendations in this report and continued monitoring by the Authority.
- 9.4 Based on the interviews it held the Panel believes that provision of mains power and air conditioning to servers is still at risk. In particular the reliance on back-up power generators which were seen as unreliable by those interviewed has to be questioned. The Panel recommends options for greater resilience to ICT power supplies be fully explored by the disaster recovery project work.
- 9.5 The Panel would also expect that the disaster recovery project work makes recommendations that would mitigate the specific risk of there being insufficient ICT specific disaster recovery plans.
- 9.6 The reliance of the Force on computer systems which are hosted on servers housed in a single site at headquarters represents a significant risk. Again the Panel recommends the disaster recovery project make recommendations to mitigate this risk. The Panel does not believe that the current arrangements to move 24 hour back-up tapes off site and have "cold" servers (i.e. with no Force software or data stored on them) delivered to HQ are viable means of continuing Force operations which are reliant on ICT. Other organisations run live or delayed back-up to other another set of servers elsewhere in their network and estate which ensure continuity of ICT if one server location is rendered inoperable.
- 9.7 It was well accepted by those the Panel interviewed that the FCCC's Temporary Back-up Facility (TBUF) is not a viable means of delivering an acceptable level of service should the FCCC's functionality be compromised. The Panel shares this view. Although the option of switching calls to a neighbouring force provides some assurance, the Panel is of the view that both in terms of another force's capacity and the sustainability of such an arrangement over a period of recovery, the mutual-aid option does not provide sufficient resilience. Greater resilience within the Lincolnshire Force should be developed. The Panel recognise this has significant capital implications.
- 9.8 The Panel therefore believes it is imperative as per the earlier recommendation that the Force consider expediting the disaster recovery projects for the FCCC and ICT provision. The Panel wishes to emphasise its view that these services and functions are absolutely critical to enabling the Force to deliver policing to the people of Lincolnshire. As noted elsewhere,

clarity around the exact remit, scope and deliverables of the disaster recovery projects for ICT and the FCCC was lacking. When this was considered alongside the absence of a timeline for this work, the Panel was not assured that sufficient action was being taken to address the identified risks.

- 9.9 It is for the Force to determine what level of risk it is prepared to accept however it is the Panel's opinion that ICT and FCCC resilience to potential threats in the form of both external and internal factors is, on the whole, currently insufficient.

**Recommendation 21: It is recommended that the disaster recovery project for ICT and FCCC gives due consideration to the following:- ICT power supply back-up, detailed ICT disaster recovery plans, increased server resilience via dual-siting, options for increasing FCCC resilience, and that the Force provide the Authority with a detailed action plan and timeline for this work, providing recommendations to the Authority on any changes to the existing capital programme.**

## **10.0 Business Continuity Requirements of the Police Authority**

- 10.1 As noted in the introduction to this report, Lincolnshire Police Authority does not currently have any formal BCM strategy or plans. The Authority recognises the risk this poses, particularly with regard to the resilience of the Secretariat, in delivering its work. Secretariat resilience currently features on the Authority's critical risk register.
- 10.2 The Panel also recognises that the Secretariat function is heavily reliant on the Force given that the Secretariat is accommodated at Police Headquarters. Accommodation, utility supplies, telephony and ICT are all provided by the Force. The Panel therefore recommends that as the Force continues its work identifying its critical functions and prioritises their continuity and recovery, it should liaise with the Deputy Chief Executive of the Authority to agree how services to the Authority are included in Force BCPs.

**Recommendation 22: It is recommended that the Force agrees with the Authority appropriate prioritisation of its provision of key services (accommodation, utility supplies, telephony and ICT) to the Authority within its critical functions and BCPs.**

- 10.3 The Panel recognises that many of the recommendations it has made to the Force should apply equally to the Authority, although given the smaller nature of the organisation some of the issues, particularly around leadership, training and culture do not present as great a challenge. However the need for a BCM strategy and resulting plan is evident.

**Recommendation 23: It is recommended that the Audit, Risk and Governance Committee consider whether the lack of business continuity and disaster recovery plans should feature on the Authority's risk registers.**

- 10.4 The Panel also recommends that the Secretariat address Business Continuity within its workplans as detailed below, subject to further discussions with Members on an agreed timeline and the resource requirements:-

**Recommendation 24: It is recommended the Authority a) maps and defines its critical functions, b) defines the desired and minimum acceptable levels of service for these functions, c) conducts business impact analyses to understand the risks to these functions, the likelihood of disruption occurring and the consequences d) prioritises the continuity and recovery of these functions e) considers and agrees appropriate control measures and f) implements a BCM policy and BCP, ensuring Officers and Members are appropriately trained, subject to an agreed timeline and resourcing.**

## **11.0 Next steps**

- 11.1 In line with the usual protocol for Authority scrutinies, the panel asks the Force to provide the Audit, Risk and Governance Committee with on-going progress updates against the recommendations outlined in this report.
- 11.2 It is also recommended that the panel conduct a formal review of the Force's progress with the recommendations and the implementing of its BCM policy no later than November 2010.

**Recommendation 25: It is recommended the Force provides the Audit, Risk and Governance Committee with on-going progress updates against the recommendations outlined in this report.**

**Recommendation 26: It is recommended this scrutiny panel conducts a formal review of the Force's progress with the recommendations and the implementing of its BCM policy no later than November 2010.**

## **11.3 Conclusions**

- 11.4 The Panel would again like to acknowledge the assistance of Force Officers and Staff which enabled this report to be compiled. Whilst recognising the challenges the Force faces in embedding robust BCM, the Panel has concluded that both an acceptance of the need and a will to do so are very much in evidence. The recommendations of the Panel inevitably reflect where the Force is in developing robust and effective BCM and the Panel hopes that these recommendations will be both constructive and timely.
- 11.5 The size of the task ahead should not be underestimated. However the panel has no doubt that if the Force meets its objectives outlined in the BC policy it will not only be better prepared to continue and recover its functions when it is adversely impacted upon, but also act as an exemplar to other Forces. The Panel looks forward to monitoring the Force's progress.

## 12.0 Recommendations

12.1 The Panel's recommendations as detailed in this report are listed below. It should be noted that they are reproduced in the order they appear in the preceding text and therefore should not be taken as having been prioritised.

**Recommendation 1:** It is recommended that the Force embeds a corporate, consistent and centrally led approach to BCM throughout the Force.

**Recommendation 2:** It is recommended that the Emergency Planning Officer be located in Strategic Development.

**Recommendation 3:** It is recommended that following formal approval of the new BC policy, the Force adopt a project management approach to managing the work necessary to deliver the project's objectives.

**Recommendation 4:** It is recommended the Force forms a business continuity management board to oversee the implementation of BC arrangements within the Force.

**Recommendation 5:** It is recommended that the Force assures itself that the oversight, ownership and management of risks relating to BC which appear on the Force risk register are properly aligned with the role of the proposed Business Continuity Management Board to ensure clarity and eliminate duplication.

**Recommendation 6:** It is recommended the Force introduces force-wide business continuity plans that address generic loss likely to impact the organisation as a whole e.g. ICT, utilities, people and estate in addition to divisional/departamental BCPs.

**Recommendation 7:** It is recommended the Force a) maps and defines its critical functions, b) defines the desired and minimum acceptable levels of service for these functions, c) conducts business impact analyses to understand the risks to these functions, the likelihood of disruption occurring and the consequences and d) prioritises the continuity and recovery of these functions. This work should then inform both Force-wide and departmental/divisional BCPs. This approach should be clearly outlined in policy and co-ordinated and led by the BC Management Board.

**Recommendation 8:** The Business Continuity Management Board review and approve departmental/divisional BCPs to ensure consistency with the above methodology and that interdependencies between parts of the Force have been properly assessed and accounted for.

**Recommendation 9:** It is recommended that the ICT and FCCC disaster recovery projects be overseen by the Business Continuity Management Board, that a clear remit and timeline prioritise this work and that any mitigation requiring capital investment be appropriately prioritised within the Capital Programme.

**Recommendation 10:** It is recommended that the Force procurement process for business critical service contracts (such as ICT support) include an assessment of the contractors' own business continuity arrangements to enable the Force to satisfy itself that contractors would be able to deliver in the event of their own operations being compromised.

**Recommendation 11:** It is recommended that the Force seek to formalise any agreements with other forces or agencies for the provision of mutual aid where this forms part of the Force's business continuity planning. Formalising these agreements should be prioritised in line with the business impact analysis referred to elsewhere in this report, i.e. focussing on the areas of greatest risk and impact first.

**Recommendation 12:** It is recommended that the Force ensure any formal protocols/agreements for mutual aid be properly documented in the relevant business continuity plans.

**Recommendation 13:** It is recommended Force business continuity plans include recovery strategies for the first 90 days following an incident which aim to return functions to preferred service levels. This should be co-ordinated by the BC Management Board.

**Recommendation 14:** It is recommended that BCM responsibilities be reflected in relevant job descriptions of police officers and staff in management and leadership roles.

**Recommendation 15:** It is recommended that the Force develop and implement a Force-wide Business Continuity training and awareness raising strategy, overseen by the Business Continuity Management Board.

**Recommendation 16:** It is recommended that the Force develop co-ordinated testing and maintenance strategies for business continuity plans, monitored by the Business Continuity Management Board. Testing should comprise live and table-top testing proportionate to the criticality of the functions individual plans cater for.

**Recommendation 17:** It is recommended the Force gives due consideration to the long term personnel resources required to deliver the objectives it is setting itself for BCM and the appropriateness of current arrangements.

**Recommendation 18:** It is recommended the Force consider expediting the disaster recovery project for the FCCC and ICT provision and that resultant recommendations requiring capital outlay be accurately factored into the capital programme and prioritised appropriately following further consultation with the Authority.

**Recommendation 19:** It is recommended that the Force continues to attend the regional business continuity forum and that they give thought to wider opportunities for collaboration once BCM internally is more robust.

**Recommendation 20:** It is recommended that the Force considers whether its generic business continuity planning offers sufficient robustness to deal with large scale redeployment or abstractions to either major incidents within Lincolnshire or to other Forces.

**Recommendation 21:** It is recommended that the disaster recovery project for ICT and FCCC gives due consideration to the following:- ICT power supply back-up, detailed ICT disaster recovery plans, increased server resilience via dual-siting, options for increasing FCCC resilience, and that the Force provide the Authority with a detailed action plan and timeline for this work, providing recommendations to the Authority on any changes to the existing capital programme.

**Recommendation 22:** It is recommended that the Force agrees with the Authority appropriate prioritisation of its provision of key services (accommodation, utility supplies, telephony and ICT) to the Authority within its critical functions and BCPs.

**Recommendation 23:** It is recommended that the Audit, Risk and Governance Committee consider whether the lack of business continuity and disaster recovery plans should feature on the Authority's risk registers.

**Recommendation 24:** It is recommended the Authority a) maps and defines its critical functions, b) defines the desired and minimum acceptable levels of service for these functions, c) conducts business impact analyses to understand the risks to these functions, the likelihood of disruption occurring and the consequences d) prioritises the continuity and recovery of these functions e) considers and agrees appropriate control measures and f) implements a BCM policy and BCP, ensuring Officers and Members are appropriately trained, subject to an agreed timeline and resourcing.

**Recommendation 25:** It is recommended the Force provides the Audit, Risk and Governance Committee with on-going progress updates against the recommendations outlined in this report.

**Recommendation 26:** It is recommended this scrutiny panel conducts a formal review of the Force's progress with the recommendations and the implementing of its BCM policy no later than November 2010.

## **13.0 Appendices**

<b>Appendix 1</b>	<b>Business Continuity Scrutiny – Scope and terms of reference</b>
<b>Appendix 2</b>	<b>Acronyms</b>
<b>Appendix 3</b>	<b>Bibliography</b>
<b>Appendix 4</b>	<b>List of existing Force business continuity policies</b>
<b>Appendix 5</b>	<b>Draft Force Business Continuity Management Policy</b>
<b>Appendix 6</b>	<b>List of Force Officers and Staff Interviewed</b>

## Appendix 1 - Scrutiny into Business Continuity Scope and Terms of Reference

Scrutiny work comprises detailed evidence based assessment of particular services or issues of local concern that can be developed or improved.

### 1. Title

#### Scrutiny into Business Continuity

##### Definitions

The British Standard on Business Continuity Management (BCM), BS25999, defines BCM as “a holistic management process that identifies potential threats to an organisation and the impacts to operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities.”

A Business Continuity Plan (BCP) identifies the impact of potential threats and formulates viable strategies which ensure continuity and/or recovery of an organisation’s operational activities.

Cabinet Office (UK Resilience) states that BCM “Must be regarded as an integral part of an organisation’s normal ongoing management process.”

The Civil Contingencies Act 2004 requires Category 1 responders, which include Police Forces, to maintain plans to ensure that they can continue to exercise their functions in the event of an emergency so far as is reasonably practicable.

The BCM duty in the Act relates to all the functions of a Category 1 responder, not just its civil protection functions. Hence the legislation requires Category 1 responders to maintain plans to deal with emergencies and put in place arrangements to warn and inform the public in the event of an emergency. But it also requires them to make provision for ensuring that their ordinary functions can be continued to the extent required. The Regulations also require Category 1 responders to put in place a training programme for those directly involved in the execution of the BCP should it be invoked.

### 2. Purpose

The purpose of this scrutiny is to contribute to the achievement and maintenance of high levels of performance, efficiency and effectiveness of the Force and Authority by conducting a scrutiny into the Force’s Business Continuity Management planning and processes.

The rationale for selecting the topic of Business Continuity is detailed below.

- **Performance:** A new Business Continuity Management policy is currently being developed (in consultation phase with DCC and Command Group). Force expectation is that adoption of the new Policy will be finalised within the next 3 months.
- **Risks:** Not having a plan or keeping it up to date and tested would mean non compliance with the Civil Contingencies Act 2004. Without appropriate BCM arrangements, the Force would not be prepared if operational activity was

adversely impacted, resulting in longer recovery times, reputational damage and increased costs. The lack of preparedness could mean areas of poor resilience are not identified and the opportunity to mitigate risk lost. A particular area to consider and build on a previous scrutiny will be the Business Continuity arrangements for the Force Communications and Control Centre (FCCC). FCCC has previously suffered from power outage (Autumn 2008), adversely impacting on operations. Business continuity features in the Force risk register.

- **Resources:** It is difficult to estimate exact costs given the cross cutting nature of the topic. The Force's objective analysis data places business continuity planning under the heading of civil contingencies that also includes contingency planning, purpose built command suites used during major/large incidents, emergencies or exercises and incident information centres. Under this heading the Force has allocated two Constables (special events and licensing) and two support staff (emergency planning officer and assistant), with a cumulative total annual cost of £143,623. There are senior staffing costs and other costs that are not reflected in this figure.
- **Impact on local communities:** The impact of this scrutiny topic is particularly significant to the communities of Lincolnshire, as it is focused on the ability of the Force to maintain a police service throughout the County if operational activity were to be adversely impacted. In such an event it would therefore link to the general public's overall perception and feelings of trust, confidence and satisfaction of policing services.
- **National Policy:** As detailed above, the Force has a statutory obligation under the Civil Contingencies Act 2004 to maintain a business continuity plan. ACPO and NPIA also recognise the need for increased resilience in police forces to be able to continue to provide critical services during an incident that could impact on a Force's own business processes.
- **Inspections:** Business Continuity forms part of the Protective Service Inspection of Civil Contingencies and Emergency Planning. This took place last year. Lincolnshire was not inspected during this phase of inspection due to the County being classified as a low risk area. The ACPO Business Continuity working group has worked closely with the HMIC to ensure that forces' business continuity plans are part of a measurable audit process. The role of the HMIC is to promote efficiency and effectiveness of police forces and, as such, ACPO's view is that business continuity plans should be measured to meet the public expectation that police forces will continue to protect them, even in catastrophic circumstances.
- The topic of Business Continuity is considered to be **cross-cutting** as it has implications across all Divisions across the Force.
- **Priorities/adding value:** The Panel and Force agree that the scrutiny will **add value** and build on planned activities within the Force; particularly the following commitments in the Policing Plan:

“In 2010/11 we will:

Ensure procedures are in place regarding our essential support activities to mitigate risks from disaster (disaster recovery and business continuity)

In 2011/12 we will:

Implement new structures and processes, to ensure that we can continue to provide a comprehensive policing service to you, if there is a technical or business failure.”

- However, the scrutiny will not **duplicate** any other work and it is hoped it will inform the achievement of these two objectives.

- The scrutiny is considered to be **timely** and **ethical** and it can be effectively **resourced**.

### 3. Objectives

The Panel aims to achieve the following:

- Understand the Business Continuity Management and Planning processes the Force has in place and identify where improvements can be made to increase the ability of the Force to maintain critical operational activities when these face disruption.

### 4. Scope

In order to maximise the benefits from the scrutiny process, the Panel plan to explore the following specific areas relating to Business Continuity:

- The Force's current and in-development business continuity management processes including planning, governance, risk management, business/disaster recovery strategy and allocation of responsibilities.
- The Force's arrangements for staff awareness and training.
- The Force's arrangements for maintaining, reviewing and updating business continuity plans and their testing.
- Identify best practice (other Forces, NPfA, ACPO, British Standards Institute)
- Consider opportunities for collaboration, both regionally with other Police Forces and locally with LAA partners and the formalisation of these through agreed protocols.
- Consider the Business Continuity Planning requirements of the Authority given the Authority's dependency on the Force for key services (e.g. ICT, telephony) and accommodation.

In carrying out the above the panel will particularly wish to consider whether critical business areas have been appropriately identified, risks and threats adequately assessed, that disaster recovery/contingency planning is sufficient and what guidance can be offered to the Force to aid planning in these areas. Priority areas suggested by the Force include FCCC, the Force estate, ICT and workforce contingencies in the event of large scale absence including chief officers.

All of the above is to be done with reference to the statutory obligations under the Civil Contingencies Act 2004 and best practice as identified by the British Standard on Business Continuity Management BS25999 and the ACPO/NPfA Guidance on Emergency Procedures.

### 5. Approach

The Chair of the Audit, Risk and Governance Committee, the Scrutiny Panel, Chief Executive, Treasurer and Deputy Chief Constable will confirm the rationale, brief and scope of the scrutiny.

#### Methodology

The scrutiny will be carried out using the following methodology:

- Undertake a literature review and conduct desk research

- Research any good practice and take advice from, Her Majesty's Inspectorate of Constabulary (HMIC), the Association of Police Authorities (APA), National Policing Improvement Agency (NPIA) and the British Standards Institute (BSI) where appropriate.
- Gather data and consider evidence-based research from Force staff/officers and carry out reality checking in order to produce a report that outlines suggestions for improvement.
- Produce a draft scrutiny report to the Audit, Risk and Governance Committee on 19 November 2009. Consider the findings and recommendations from the Panel at the meeting, which will include questions to relevant Force staff/officers (maximum one hour time slot within Committee agenda).
- Revisit progress made by the force in implementing and embedding the Business Continuity Policy and resultant Plan(s) in 12 – 15 months.

NOTE: there is an expectation that all relevant Force officers/staff and the lead Chief Officer will be present at the meeting to enable effective discussion and debate.

- If necessary, arrange a follow up meeting 6 – 8 weeks following the Audit, Risk and Governance Committee to assimilate and rationalise information following the Committee's consideration of the scrutiny report.

## **6. Derivation**

- Information and evidence will be sourced from Force staff and officers at both strategic and operational level. On a strategic level, the Deputy Chief Constable Neil Rhodes is the Chief Officer lead in this business area. However there are significant priority areas under the command of Assistant Chief Constable (Protective Services), Alec Wood, including Emergency Planning and the FCCC, with BCUs the responsibility of ACC Keith Smy.
- Source information through the National Policing Improvement Agency (NPIA), the Association of Chief Police Officers (ACPO), Her Majesty's Inspectorate of Constabulary (HMIC), the Home Office, the Association of Police Authorities (APA), and the British Standards Institute (BSI).

The key contact points in the Force have been suggested as:

- Planning Officer, Emergency Planning (Ian Watkins)
- Project Manager for disaster recovery (Ian Rushton)
- Head of Force Communications and Control Centre FCCC (C/Insp Keith Owen)
- Head of Information, Communication and Technology (Ian McCorrison)
- Director, Human Resources (Sue Scott)
- Director, Finance and Administration (Peter Steed)
- Head of Strategic Development (Nancie Shackleton)
- Head of Operations (Ops) Support (C/Supt Terry Hackett)/Deputy Head of Operations (Ops) Support (Supt David Lynch)
- Divisional Commanders (C/Supt Carl Langley, C/Supt Dave Hayward, C/Supt Russ Hardy)
- Deputy Chief Constable Neil Rhodes
- Assistant Chief Constable (Protective Services) Alec Wood
- Assistant Chief Constable (Safer Neighbourhoods) Keith Smy

## 7. Composition

The scrutiny report will include the following chapter headings:

- *Introduction*
- *Background*
- *Management and planning arrangements*
- *Communication and training arrangements*
- *Testing and updating arrangements*
- *Resourcing*
- *Challenges*
- *Risks*
- *Recommendations*
- *Conclusion*
- *Appendices*

## 8. Format

The Scrutiny Panel will produce a report for submission to the Audit, Risk and Governance Committee.

## 9. Exclusions

To ensure that the scrutiny remains focussed and deliverable within time and resource constraints, the Panel will not be able to consider all aspects of Business Continuity and contingent/interrelated areas.

The following exclusions will apply:

- An active test of the Force's Business Continuity Plan
- Planning related to Force operational response to emergencies or major incidents regardless of their cause.

Significant work is being undertaken by Nancie Shackleton around contingency planning for the potential effects of swine flu. This work is well advanced. This should not be excluded from the scrutiny, but it maybe that there are other areas where the panel could add greater value and so will prioritise their work and its depth accordingly.

## 10. Timescales

<b>Action</b>	<b>Deadline date</b>
Topic agreed	21 May 2009
Expression of interest requested	24 July 2009
Panel formed	31 July 2009
Produce scope and background research (including initial meeting with DCC and ACC)	7 August 2009
Agree terms of reference with Force	August 2009

Conduct Fieldwork September 2009	August,
DCE start to write report by at least 2009	28 September
Final report emailed to Panel for comments	<b>9 October 2009</b>
Deadline for Panel to return comments	16 October 2009
DCE make amends/run passed CE 2009	16 - 21 October
Final report emailed to Force for comments	21 October 2009
Deadline for Force to return comments	<b>28 October 2009</b>
DCE to forward to CE/T final clearance	2 November 2009
CE/T clear papers deadline	4 November 2009
Meeting to finalise papers	4 November 2009
Despatch papers 2009	12 November
Audit, Risk and Governance Committee Meeting date 2009	19 November
Follow up meeting if necessary	6 – 8 weeks later

#### **11. Membership**

Mrs Angela Crowe JP	Audit, Risk and Governance Committee	Panel Lead
Mr Paul Przystlak	Audit, Risk and Governance Committee	Panel Member
Mr John Atter	Community and Partnership Committee	Panel Member
Miss Ginny Mason	Research & Performance Officer	
Mr Howard Hunt	Deputy Chief Executive	
Ms Deborah McGovern	Chief Executive	
Ms Julie Flint	Treasurer	

#### **12. Resource Implications**

Member expenses (to the end of September 2009):

Attendance at 6 meetings (18 ½ hours in total) x 3 Members) =	£1110.00
Travel time expenses and mileage costs (based on 6 meetings) =	£1411.20
Total Approximately	<b>£2521.20</b>

- DCE/RPO time (approximately 2 - 3 days/week for the scrutiny period)/Secretariat time
- Force opportunity costs (staff/officers attendance at panel meetings)

#### **13. Bibliography/Additional Information**

The following is taken from the ACPO/NPIA Guidance on Emergency Procedures 2009:  
<http://www.acpo.police.uk/asp/policies/Data/Emergency%20Procedures%202009.pdf>

An emergency or major incident is likely, by its definition, to place a significant burden on the police. A continued policing provision is still required to be delivered, both in the area directly affected and across the rest of the force area. This requirement is one of the strategic objectives in maintaining the rule of law. The effectiveness of any response to

an incident can be reduced where there is a partial or full breakdown in law and order in the area concerned.

Business Continuity Management is the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable pre-defined level. BCM planning should be aimed at maintaining critical activities, and response to an incident must take into account the likelihood and impact of the loss of one or more critical activities or critical infrastructure of the force.

Police forces, as category 1 responders, have a legal duty under the Civil Contingencies Act 2004 to prepare business continuity plans to cover the loss of critical activities. Critical activities are those activities which have to be performed in order to deliver the key products and services which enable an organisation to meet its most important and time sensitive objectives. The plan should cater for circumstances where there is a sudden and significant loss of infrastructure or facilities, for example flooding, major fire or loss of information technology systems. It should also cater for a scenario where the activities of the police force have to be collapsed to concentrate on critical activities, for example during an emergency where staff absenteeism rises severely or during a major incident where a large number of police personnel are deployed.

The business continuity plan should detail the business continuity management structure and processes to be adopted at times of crisis. A senior police officer or police staff manager should be appointed as the business continuity manager, operating at a strategic level. The business continuity manager should have a clear line of communications with the Gold Commander, and may sit on the Strategic Co-ordinating Group, although this may not always be appropriate because of the differing focus of business continuity as opposed to the control and command of the emergency or major incident.

The business continuity manager should convene a team of key personnel to implement the business continuity process. The plan should identify the resources, services and actions required to maintain critical activities and, if they are lost, to restore them within a defined timescale. The key to business continuity management is resilience against disruption, and while it is internally focussed, it should take account of interdependencies with other organisations that may be affected by similar disruption at the same time.

### **Backing-up the policing basics**

**(Article from “Public Service Review: Home Affairs Issue 16” - Wednesday, October 03, 2007)**

Mike Bowron, Commissioner of the City of London Police, ACPO, explains why the implementation of business continuity is as important to routine management within the Police Service as it is to critical activity in the face of emergency.

The Civil Contingencies Act 2004 places a responsibility on police forces to have in place emergency plans and business continuity management arrangements.

The Police Service is classed as a Category 1 responder and, as such, the Service needs to maintain plans to ensure that it can continue to exercise its functions in the event of an emergency so far as is reasonably practicable.

An emergency, for the purpose of the Civil Contingencies Act, is defined as an event or situation that threatens serious damage to human welfare in a place in the UK; an event or situation that threatens serious damage to the environment of a place in the UK; or war or terrorism that threatens serious damage to the security of the UK.

For the Police Service, this means being able to deal with an emergency as well as manage day to day routine business. The police will normally co-ordinate the activities of those responding at and around the scene of a land-based sudden impact emergency. The key priority is the saving and protection of life; however, care will also be taken to safeguard evidence for subsequent enquiries and, possibly, criminal proceedings.

As well as managing all of these elements in the event of a major incident, the Police Service has to continue with attending other emergency calls and reports of crime, as well as neighbourhood policing.

The Association of Chief Police Officers (ACPO) business continuity working group has been set up to provide guidance and information to support forces with business continuity plans already in place, with the main aim of developing a culture and awareness at a senior level in forces for the need for such plans. This overarching aim also includes working closely with Her Majesty's Inspectorate of Constabulary (HMIC) to influence a future audit process, determining appropriate Police Service focused training for business continuity, the sharing of Best Practice and BC issues through regional forums, and providing BC guidance for forces.

Regardless of the requirements of the Civil Contingencies Act, every police force needs to ensure that it can continue to deliver key services to their communities during a period of disruption. Despite the publicity that major incidents attract, it is often the mundane incidents that can cause operational disruption.

Police forces throughout the UK have suffered from burst internal water pipes, fires, flooding from sewerage, shortage of skilled staff, failures in IT, telecommunications and power. Major crimes, such as the Soham murders, have resulted in the redirection of staff away from front line operations. All of these incidents have put pressure on the police's service to the public.

Business Continuity Management enables police forces to prepare for any disruption and ensure that key services are delivered to the community regardless of the disruption. The working group for BC has developed a lot in the past year; for one, there is now a comprehensive understanding of how we can assist forces in their plans – we work closely with the Civil Contingencies Secretariat to ensure we are developing our guidance in line with what is expected of Category 1 responders.

The working group is also keen to develop the understanding that business continuity does not just come into effect after a major incident but can also be required, for example, when road closures are necessitated, meaning that a large police presence is needed to manage diversions, etc.

It is essential that forces understand that providing a good response to all incidents that require an increased use of resources, and not only those defined as emergencies through the Act, can be a useful mechanism in tackling everyday issues. To this end, the working group has been ensuring that there is a clear idea at least of what the critical activities are for the Police Service to deliver during such an incident, and we are able to disseminate these thoughts through the regional forums to forces.

All forces now view their business continuity plans as essential to their critical activity; the Metropolitan Police Service (MPS) is a force spanning a vast area that has such plans in place.

An example of this in practice was the 7/7 bombings, which posed major challenges, significant staff abstraction and disruption to travel for many MPS staff. It proved that a major event can occur at any time and anywhere, and can vary in its size and nature.

However, no matter what the incident, the MPS, like any force, must be prepared to not only deal with it, but also have business continuity plans in place to continue to deliver all the essential critical activities associated with daily policing business. Following 7/7, a review of the forces' approach to business continuity was carried out to ensure that the planning and management were appropriately focused, and that there was clarity over what the critical activities of the MPS were.

Norfolk Constabulary, although covering a smaller area than the Metropolitan Police, has also set in place business continuity plans to ensure that they can keep daily business going during a major incident.

They have used workshops, training and exercises to ensure that the plans are communicated effectively and that they are a leading partner in the Community & Economic Resilience Sub-Group of the Norfolk Resilience Forum, which aims to develop an integrated strategy for the effective promotion of business continuity.

The national BC forum working group has also formed nine regional BC groups, which are able to ensure an overview of activity throughout the 42 forces in England and Wales.

The regional groups exist to share good practice and exercise together locally, regionally and nationally, ensuring that the plans that forces have work in real-time situations. The forum has also sponsored two conferences on business continuity, which were held at the Emergency Planning College in Easingwold. Representatives from forces attended the conferences to find out about business continuity plans and to share ideas. In addition to this, regional forums have also been organised, the most recent of which was in Hampshire for South East forces.

The BC working group has also worked closely with the HMIC to ensure that forces' business continuity plans are part of a measurable audit process. The role of the HMIC is to promote efficiency and effectiveness of police forces and, as such, business continuity plans should be measured to meet the public expectation that police forces will continue to protect them, even in catastrophic circumstances.

The collaboration between ACPO and the HMIC to support forces in their work on contingency plans for the provision of services to the public is of high importance because it underpins the continuing provision of fundamental police services.

Howard Hunt  
E:\Scrutiny\Business Continuity Scope final version 1.0.doc

## **Appendix 2 – acronyms**

ACC	Assistant Chief Constable
ACPO	Association of Chief Police Officers
BC	Business Continuity
BCM	Business Continuity Management
BCP	Business Continuity Plan
BCU	Basic Command Unit
BSI	British Standards Institute
CCA	Civil Contingencies Act
DCC	Deputy Chief Constable
FCCC	Force Communications and Control Centre
HMIC	Her Majesty's Inspectorate of Constabulary
HQ	Headquarters
ICT	Information Communications Technology
LAA	Local Area Agreement
NPIA	National Policing Improvement Agency
PDR	Performance and development Review
TBUF	Training and Back-up Facility

### **Appendix 3 – Bibliography**

ACPO/NPIA Guidance on Emergency Procedures 2009  
<http://www.acpo.police.uk/asp/policies/Data/Emergency%20Procedures%202009.pdf>

British Standard on Business Continuity Management BS25999 (British Standards Institute)

Business Continuity Guidelines – dealing with a pandemic flu (Aviva Risk Management Solutions)

Business Continuity Plan template Guide – Walsall Council  
[http://www.walsall.gov.uk/index/business\\_continuity\\_plan\\_template\\_guide.htm](http://www.walsall.gov.uk/index/business_continuity_plan_template_guide.htm)

Business Resilience – A Guide to Protecting Your Business and Its People (The Fire Protection Association 2005)

Civil Contingencies Act 2004  
[http://www.opsi.gov.uk/acts/acts2004/ukpga\\_20040036\\_en\\_1](http://www.opsi.gov.uk/acts/acts2004/ukpga_20040036_en_1)

Guidelines for Business Continuity Planning (Aviva Risk Management Solutions)

An Introduction to Business Continuity Planning (Aviva Risk Management Solutions)

Telecommunications and Business Continuity (Aviva Risk Management Solutions)

#### Appendix 4 - List of existing Force business continuity policies

Business Continuity	Crisis Management Plan	Last Revision Date: 16 July 2009
Business Continuity Activation Plan Pandemic Influenza	West Division	Last Revision Date: 16 July 2009
Business Continuity Activation Plan Pandemic Influenza		Revision Date: 23 July 2009
Business Continuity Plan	Business Services	Plan Review Date: 31 March 2010
Business Continuity Plan	Crime Support	Plan Review Date: January 2010
Business Continuity Plan	Human Resources	Plan Review Date: August 2009
Business Continuity Plan	Information Management Unit	Plan Review Date: 1 May 2010
Business Continuity Plan	Operations Supports	Plan Review Date 3 October 2009
Business Continuity Plan	South Division Administration (Grantham Station)	Plan Review Date 10 October 2010
Business Continuity Plan	Strategic development Department	Plan Review Date: August 2010
<i>Business Continuity Plan</i>	<i>West Division</i>	<i>Last Review date: 16 July 2009</i>
<i>Business Continuity Plan</i>	<i>West Division Administration</i>	<i>Last Review date: 13 July 2009</i>
<i>Business Continuity Activation Plan</i>	<i>Finance and Admin Directorate – Finance Section</i>	-
<i>Business Continuity Activation Plan Pandemic Influenza</i>	<i>Finance and Admin Directorate – Finance &amp; Procurement Section</i>	-
<i>Business Continuity Plan</i>	<i>Fleet Management</i>	<i>Plan Review Date: to be ascertained</i>

#### Out dated Business Continuity Plans in Force

Business Continuity	Crisis Management Plan	Plan Review Date: 7 December 2008
Business Continuity Plan	FCCC	Review Date: 1 November 2006
Business Continuity Plan	South Division	Plan Review Date: 31 July 2006
Business Continuity Plan	Criminal Justice Support, Criminal Justice Units	Plan Review Date: 31 March 2006
Business Continuity Plan	Criminal Justice Support, Crown Court Liaison	Plan Review Date: 31 March 2006
Business Continuity Plan	Criminal Justice Support, Central Ticket Office	Plan Review Date: 31 March 2006
Business Continuity Plan	Criminal Justice Support, Viper Unit	Plan Review Date: 31 March 2006
Business Continuity Plan	Firearms Licensing Department	Plan Review Date: 14 March 2007
Business Continuity Plan	Information and Communications Technology	Plan Review Date: 1 November 2005
Business Continuity Plan	East Administration	Plan Review Date: 31 March 2006

Business Continuity Plan	Finance and Administration Department, procurement Unit	Plan Review Date: 10 July 2009
Business Continuity Plan	Property Management	Plan Review Date: 13 January 2004

Copies of these documents are held by the Authority secretariat

## Appendix 5



# LINCOLNSHIRE POLICE

### 1. POLICY IDENTIFICATION SHEET

*This policy has been drafted in accordance with the principles of human rights legislation, public disclosure is approved unless where otherwise indicated and justified.*

<b>POLICY TITLE:</b>	BUSINESS CONTINUITY MANAGEMENT
<b>POLICY REFERENCE NO:</b>	DRAFT 2 7/4/09

<b>POLICY OWNERSHIP:</b>	
<i>Portfolio / Business-area Owner:</i>	DCC RHODES
<i>Department Responsible:</i>	OPERATIONS SUPPORT
<i>Person Responsible:</i>	EMERGENCY PLANNING OFFICER
<i>Links or overlaps with other policies/strategies:</i>	
Organisational Risk Management Policy (PD122(1))	
Strategic Plan 2008 to 2011	
ICT Strategy 2004 – 2008	
PNC Strategy 2007 - 2010	

<b>POLICY IMPLEMENTATION DATE:</b>
<b>POLICY REVIEW DATE:</b>

## 2. **POLICY STATEMENTS/INTENTIONS**

### 2.1 *The principles and scope of the policy*

The Chief Constable of Lincolnshire Police is a Category 1 Responder as defined by the Civil Contingencies Act 2004 (CCA) and has duty to maintain plans to ensure that they can continue to perform their functions in the event of an Emergency, so far as is reasonably practicable. This duty relates to all the functions of a Police Force, not just its civil protection functions.

The Chief Constable, as part of the Tri-Partite arrangements responsible for the provision of an efficient and effective Police Service in Lincolnshire also has a wide range of statutory and other duties and responsibilities placed upon them intended to ensure such a service is provided. The staff and other resources employed by or on behalf of Lincolnshire Police perform functions intended to enable the Chief Constable to meet their responsibilities.

Lincolnshire Police will strive to meet all the legal duties placed upon it by the CCA and will develop, maintain and implement plans that ensure the Force is able to continue to perform its functions so far as is reasonably practicable in the event of an Emergency as defined by the CCA and where possible, a wider range of disruptive challenges than those covered by the CCA.

Lincolnshire Police will also seek to adopt good practice as described within the statutory and non-statutory guidance issued under the CAA and by authoritative bodies such as Cabinet Office and HMIC.

In particular in relation to Business Continuity Management the Force will adopt the principles described within British Standard 25999 – Part 1.

This policy is applicable to the whole Force and to persons or organizations undertaking Critical Activities on behalf of the Force.

The scope of this policy will be limited. The Deputy Chief Constable as chair of a Business Continuity Management Group will be responsible for determining the scope of BCM by identifying the activities that enable delivery of the key products and services that support the organization's objectives, obligations and statutory duties (these will be called Critical Activities). Determination of what is 'key' should be informed by and consistent with the results of detailed Business Impact Analysis. Risks relating to activities not to be covered by this Policy will be managed by alternative means. All risks relating to Critical Activities with a maximum tolerable period of disruption of greater than 90 days will be dealt with under arrangements imposed by the Organisational Risk Management Policy. It is also expected that some risks initially identified by processes supporting the Organisational Risk Management Policy may need to be referred for management using Business Continuity Management processes.

## 2.2 *The aim of the policy*

To ensure that, the Chief Constable meets their statutory responsibilities relating to Business Continuity, under the Civil Contingencies Act 2004 and is able to continue to perform their functions in the face of all other reasonably foreseeable disruptive challenges.

## 3. **INTRODUCTION/LEGAL BASIS**

### 3.1 *The origins/background information*

Many police functions are legal requirements but others are functions undertaken voluntarily by the Force in order to achieve its strategic aims. The Police Act 1966 directs that a police force shall be under the direction and control of the chief constable. In discharging his functions, every chief constable shall have regard to the local policing plan issued by the police authority for his area.

Police forces perform a range of functions that are intended to uphold the law fairly and firmly; to prevent crime; to pursue and bring to justice those who break the law; to keep the Queen's peace; to protect, help and reassure the community; and to be seen to do this with integrity, common sense and sound judgement.

They share with other organisations common objectives including the protection and preservation of life, human welfare, national security, community safety, property and the environment.

Historically the Police are regarded by the public as one of the key organisations that will respond to assist them in crisis situations no matter what the cause. There is a high level of expectation that they will continue to function effectively in the face of the most challenging circumstances. The added difficulty is that the Police, along with other Category 1 Responders, are expected to do this whilst responding to the effects of any crisis at the same time. Finally, during times of crisis, the Police will also be expected to coordinate, and sometimes control the response of other organisations to any crisis classed as an Emergency by the CCA.

It is accepted good practice in both public service and private sector businesses that organisations should expect crisis situations to arise and have plans and procedures in place that enable them to continue to function effectively. In the commercial world effective business continuity arrangements are an economic necessity. They are in place to ensure the organisation continues to be profitable in the long term. In the past the Police, other Emergency Services and critical public service organisations have voluntarily accepted the requirement to adopt some business continuity principles in order to maintain

their capabilities. The Civil Contingencies Act 2004 has made it a legal requirement that appropriate business continuity arrangements are in place within each Category 1 Responder Organization.

The Cabinet Office have issued a document entitled 'Expectation and Indicators of Good Practice Set - The Civil Contingencies Act (2004), its associated Regulations (2005) and guidance, and the Resilience Capabilities Programme'. This document is intended to clarify what is expected of Category 1 and 2 responders in England and Wales in relation to the duties within the Civil Contingencies Act 2004; the associated Contingency Planning Regulations 2005 and guidance and the Resilience Capabilities Programme.

HMIC have also produced the Specific Grading Criteria to be used in Inspections during 2008 and 2009 relating to Force's compliance with the Civil Contingencies Act 2004.

In late 2007 the British Standards Institute produced 'BS25999 Part 1 – Code of Practice' which is now accepted as the good practice guidance, which should be followed regarding implementation of Business Continuity principles in organizations.

A key element and expected feature of effective Business Continuity Management is the existence of an appropriate policy, which defines the set-up activities for establishing a business continuity capability and the arrangements for ongoing management and maintenance of the business continuity capability.

### **3.2 *Motivators/Driving Forces***

Chief Officers and the Police Authority have responsibilities to maintain an effective and efficient police service in their area. Alongside the Home Secretary they are required to deliver a wide variety of policing services to agreed standards. Though disruptions in service delivery are anticipated the Force would not be regarded as efficient or effective if in the face of disruptive challenges, it was unable to continue delivery of service to an acceptable level. What is acceptable will depend to some extent on the circumstances and acceptance indicated by public opinion, public or judicial enquiries or inspectorate bodies such as HMIC. The absence of evidence of appropriate Business Continuity Management and planned responses to business interruptions would be likely to attract criticism from those judging force performance and may expose the force to risks such as loss of reputation, financial penalties or punitive action against individual commanders.

The HMIC are the inspectorate body tasked with monitoring and reporting upon Force compliance with the legal standards and indicating the level of effectiveness and efficiency by comparing our performance and practices against recognised good practice, agreed standards. The Cabinet Office also monitor and report on the perceived capability of Police Forces to respond effectively to any Emergency including the perceived capability to maintain appropriate levels of service whilst responding to the Emergency. Inspections and monitoring processes include elements specifically relating to Force

compliance with the CCA and accepted good practice regarding Business Continuity Management.

The legal requirements have been made, the guidance regarding good practice and indicators of appropriate standards have been agreed and supplied to the Force by Cabinet Office and HMIC.

It is now appropriate to ensure Force Policy and working practices meet the legal requirements and where possible and appropriate reflect good practice.

### 3.3 *General Principles of the Policy*

The Business Continuity Management objectives of Lincolnshire Police will be:

- To produce and maintain a graded set of Critical Activities (including those undertaken by other persons or agencies on behalf of the force). There will be three Grades numbered 1 to 3 with Grade 1 Activities being those activities creating the greatest risks within the shortest timescales.
- To produce and maintain appropriate performance indicators and guidelines regarding acceptable minimum standards of performance related to each Critical Activity.
- To agree the maximum tolerable period of disruption for each Critical Activity.
- To produce a list of Critical Activities for which Business Continuity Strategies are to be applied, which ensure Critical Activities are maintained at or above acceptable minimum standards within the agreed maximum tolerable period of disruption for each activity.
- To produce and maintain any Business Continuity Strategies required and where necessary a suite of Incident Management, Business Continuity or Business Recovery Plans relating to those Critical Activities where the BC Strategy indicates these are appropriate.
  
- To indicate recommended alternative loss mitigation or risk treatment measures that should be applied to remaining identified risks.

The Deputy Chief Constable will be responsible for implementation, development and review of this Policy. The Policy will be reviewed at least every 2 years or sooner if required.

The Deputy Chief Constable will appoint persons as appropriate to be responsible for implementation and maintenance of a Business Continuity Management Board. This 'Board' will be responsible for:

- Implementing Business Continuity arrangements within the Force.
- Overseeing implementation and maintenance of Business Continuity Management arrangements.
- Approving strategies or plans produced on behalf of the board.
- Achieving the Business Continuity Management Objectives of the

Force.

- Producing and maintaining auditable evidence of the implementation and maintenance of the BCM Programme (See Para 5.5 of BS 25999).
- Monitoring and responding to changes in statutory requirements, indicated minimum standards set by authoritative bodies and identified good practice. This includes monitoring of this policy.

The Chair of the Business Continuity Management Programme Board will be the Deputy Chief Constable or other person appointed by them.

The guidance in the following documents will be taken into account when deciding the scope of BC arrangements and acceptable minimum standards to be achieved.

- Cabinet Office – Expectations and Indicators of Good Practice – The Civil Contingencies Act 2004, its associated Regulations (2005) and Guidance, and the Resilience Capabilities Programme.
- HMIC Specific Grading Criteria – Civil Contingencies 2008/2009.

The aim should be to at least meet and preferably exceed the implied standards.

The Chair of the Business Continuity Management Board will be responsible for allocating responsibilities for the management of specific tasks or areas of work related to Business Continuity Management to individuals as appropriate. Where necessary persons representing organizations undertaking Critical Activities on behalf of the force may be required to participate in Force Business Continuity Management processes and/or take responsibility for specific tasks or areas of work relating to Business Continuity Management.

Allocation should take into account the nature, scale, complexity, geographic location of and criticality of business activities, Force culture, dependencies and operating environment. Division of responsibility along Divisional or Departmental boundaries may not always be appropriate due to the complexity and interdependence of the organization. There are very few areas of the force that undertake critical activities that can operate independently. It will therefore be necessary to establish processes that enable effective Business Continuity Management of all Critical Activities but avoid unnecessary duplication of effort or conflict.

The graded set of Critical Activities will initially be produced and approved by the 'Board' within 1 month of the implementation of this policy using their professional judgement. The 'Board' will then implement a rolling program of work to validate and where necessary amend the set using the Business Impact Analysis methodology described in BS 25999 – Part 1. The program of work will ensure all aspects of Force Activity are reviewed within a 5 year cycle. The 'Board' will decide the priority and timescales for the Business Impact Analysis Programme.

The arrangements ensuring Critical Activities are maintained at or above acceptable minimum standards within the agreed maximum tolerable period of disruption for each activity will be based upon evidenced risk assessment.

Strategies and Plans produced as a result of this policy will use Template Designs approved by the BCM Board.

The Deputy Chief Constable and BCM Board will be provided with appropriately skilled staff to support the implementation and maintenance of this BCM Policy.

### 3.4 *Legal Basis*

This policy imposes duties and responsibilities solely upon persons employed by or on behalf of Lincolnshire Police. Persons can be lawfully required to undertake lawful tasks as part of their contracted employment. Undertaking the tasks required to comply with this policy will in most cases already be covered by clauses within existing contracts. Where necessary the Force has the legal authority to re-negotiate contracts, job descriptions and remuneration.

The Force has a statutory duty imposed by the CCA to maintain plans to ensure that they can continue to perform their functions in the event of an Emergency, so far as is reasonably practicable. This duty relates to all the functions of a Police Force, not just its civil protection functions.

The Civil Contingencies Act 2004 allows for Regulations and Guidance to indicate how the duty should be undertaken and allows for an inspectorate body to be appointed to establish whether the legislation is being complied with. In the case of Police Forces the inspectorate body appointed is HMIC. The HMIC have published Specific Grading Criteria indicating some of the measures they will apply to assessing Force's compliance with the legislation.

Where the Force wishes to impose a duty upon a supplier of goods or services it will be necessary to do so by including the requirements in the terms and conditions of lawful contracts. Where contracts already exist without such terms and conditions it will be necessary to enter into voluntary agreements or to terminate current contracts and re-negotiate new contracts of an appropriate nature.

### 3.5 *Human Rights Considerations/Articles Engaged*

The implications of the Human Rights Act have been considered. Nothing in this Policy impacts upon or conflicts with the Articles of the act. Implementation of the Policy may assist the organisation by identifying work that would not be regarded as 'forced or compulsory labour' in accordance with Article 4.3(c).

It is possible that persons producing strategies of plans as a result of this Policy will consider actions, which may conflict with the act. Each proposed

plan of action will need to be considered individually.

#### 4. **APPENDICES**

##### *List*

##### *all*

##### *Appendices*

Examples are: Risk assessments and health and safety considerations; Specific instructions, tactics, methods, practices and procedures; Individual roles and responsibilities; Related protocols, practices or service agreements with other agencies; Administration

#### 5. **IMPLICATIONS OF THE POLICY**

##### 5.1 *Financial Implications/Best Value*

It is anticipated the Business Continuity Management Board would be formed from currently serving employees including representative Chief Officers, Divisional Commanders and Departmental Heads. These members of staff already complete work related to Business Continuity Management. This policy will result in them doing the same work within an adapted framework.

It is expected that a significant amount of work will be involved in the initial stages of implementing this policy. Business Impact Assessment and the production and maintenance of Business Continuity Plans can be time consuming and requires staff with relevant expertise to complete the work. Once effective BCM Policies, Procedures and Plans are in place and embedded the workload will reduce to that required for ongoing maintenance. The Force has choices regarding how it manages completion of this work. Work may be achieved by the appointment of additional staff for this purpose or by the re-deployment or re-tasking of current staff.

The Business Continuity Management Programme Board will be responsible for making decisions about which of these methods is most appropriate and for producing a Business Case for any additional resources required for specific projects or for ongoing development, implementation and maintenance of the Business Continuity Management related activity.

It is expected compliance with this policy will be viewed as an enhancement to Best Value arrangements. The Policy is in line with the British Standard for Business Continuity Management. Effective implementation will lead to more efficient use of the workforce and other resources.

##### 5.2 *Human Resources/Training*

Members of the Business Continuity Management Board will require training to ensure they are familiar with this Policy, the BCM Management Process

described in BS 25999 and with relevant indicators of good practice. It is anticipated this training can be delivered in two stages of approximately 6 hours pre-reading followed by a 6 hour (1 day) formal presentation. The training may be delivered using current force resources but is probably best delivered by professional specialist Business Continuity Management trainers. Approved /accredited training is available from a variety of sources, approximate costs being £600 per person.

The person or persons required to undertake the work of implementing and maintaining the BCM Policy and producing BC Plans should have the skills and knowledge relevant to 'NOS - CC AD1 Develop, maintain and evaluate business continuity plans and arrangements'. This will involve identifying a person or persons who have relevant skills and knowledge or providing appropriate training. Training will generally involve attendance on a series of courses provided by recognised bodies such as the Emergency Planning College or other accredited training providers. In total approximately 12 days training spread over 4 weeks combined with relevant experience will be required. It may take up to a year to complete such training and induction. Alternatively it may be felt appropriate to recruit a person or persons with the relevant skills into the force.

Persons required to maintain BC Plans should have received appropriate training. It is expected this would be provided by the person or persons required to produce the plans. Alternatively a minimum 4 hours of formal training will be required followed by 2 hours of related private study.

Persons with key roles within any BC Plans produced will require initial training regarding their role within the plan followed by regular updates / exercises to refresh knowledge and provide opportunities for them to practice their skills. It will be necessary for each BC Plan to contain a Training and Exercising element setting out the training and exercise requirements. It is not possible to predict accurately what the requirements of each plan may be but it should be expected that initial training may take approximately 4 hours followed by 2 hours refresher training and 2 hours exercising during each review period (usually annual).

### 5.3 *Corporate/Business Plan*

Risks associated with the achievement of the Policing Plan and individual departmental plans are managed as part of the process.

### 5.4 *Risk Management*

The BCM Board will be responsible for identifying risks to the BCM Process and either managing these or referring them to alternative risk management processes for management in accordance with the Organisational Risk Management Policy.

The key risks to the implementation and continued compliance with the policy

are:-

- Failure to ensure ownership of the policy at 'executive' level.
- Failure to appoint appropriately skilled persons with sufficient authority to membership of the Business Continuity Management Board.
- Failure to appoint appropriately skilled person(s) who have adequate time and resources available to manage the day to day implementation and maintenance of the BCM Policy and production and maintenance of BC Plans
- Failure to include compliance with the BC Policy within the appraisal. Reward and recognition processes used within the Force.
- Failure to make those deemed responsible for delivery of elements of the plan accountable for successful delivery.

### 5.5 *Health and Safety*

No significant risks to health and safety are created by compliance with the policy.

### 5.6 *Diversity*

The policy has been assessed as low impact for diversity impact and has no specific implications for diversity issues.

### 5.7 *Every Child Matters*

This issue has been considered and no negative impact on the welfare of children can be identified. It is anticipated that at times when the Force is required to respond to Major Incidents, Emergencies or other Business Interruptions the policy will have a positive impact on the welfare of children by ensuring the Critical Activities which impact upon ensuring the welfare of children will not be subject to undue disruption.

### 5.8 *Crime and Disorder Act*

By increasing the resilience of the Force to disruptive challenges, compliance with this policy will have a positive effect by increasing the Forces ability to reduce crime and disorder. Though resources will be consumed implementing the policy it is anticipated that the net effect will be to ensure more resources are released for the purpose of dealing with crime and disorder, by organised effective responses to disruptive challenges, than are consumed by implementation of the policy.

The improved capacity of the force to deal with extreme peaks of demand and to retain a capability to deal with normal policing whilst responding to Major Incidents and Emergencies will result in significant positive benefits.

### 5.9 *Internal Policy/Strategy Links*

Corporate Risk Management Policy is closely linked in that it imposes a process to be used to manage risks to the organisation. These risks may include some, which threaten the force ability to implement the Policing Plan and individual departmental plans or meet other legal duties. This policy however does not adequately cater for the management of Business Continuity risks. The risk management processes imposed by each policy will need to interact with each other effectively. There should be clear communication between the individuals managing both processes and ongoing clarity regarding allocation or responsibility for the management of specific risks.

The ICT and PNC and Operational Support Strategies specifically refer to and allocate responsibilities for managing Business Continuity related to their subject areas. These will need taking into account during implementation of this policy in order to avoid confusion or conflict.

Operational Support Strategy allocates responsibilities for 'Emergency Planning'. This includes management of the business continuity risks likely to result in or arise from an Emergency as defined by the CCA. Implementation of this policy should be regarded as part of the process of managing these risks. Emergency Plans produced to show how the force will respond to risks likely to result in an Emergency will include measures to maintain business continuity. It will be necessary to ensure sets of plans complement each other.

#### 5.10 *Consultation*

Ongoing.

#### 5.11 *Publication*

The policy will be published on the Force internet and intranet.

### 6. **PROMOTION/DISTRIBUTION**

Initial promotion of the Policy will be managed by the Emergency Planning Officer via the Intranet, Routine Orders, Chief Officer Group, Operational Commanders Group and Strategic Development Group.

Once established the BCM Board and any staff appointed to support them will be responsible for promotion and distribution of the policy and related material.

### 7. **MONITORING/REVIEW**

The policy will be monitored by the BCM Board as part of the BCM process.

## **Appendix 6 – List of Force Officers and Staff Interviewed**

Deputy Chief Constable Neil Rhodes

Assistant Chief Constable Keith Smy

Assistant Chief Constable Alec Wood

Chief Superintendent Russ Hardy

Chief Superintendent Dave Hayward

Chief Superintendent Terry Hackett

Chief Inspector Keith Owen

Director of Finance Peter Steed

Head of Strategic Development Nancie Shackleton

Head of ICT Ian McCorrison

Head of HR (Strategy) Liz Hurford

Head of Programme and Planning Nicky Prutton

Project Manager for Disaster Recovery Ian Rushton

Emergency Planning Officer Ian Watkins