POLICY

NORFOLK CONSTABULARY Our Priority is You

SUFFOLK CONSTABULARY Taking pride in keeping Suffolk safe

BUSINESS CONTINUITY

Policy owners	Head of Protective Services Specialist Operations
Policy holder	Contingency Planning
Author	Business Continuity Manager

Policy No.	132

Approved by

Legal Services	✓
Policy owner	✓

Note: *By signing the above you are authorising the policy for publication and are accepting accountability for the policy on behalf of the Chief Constable.*

Publication date	9 December 2014
Review date	9 December 2018
APP Checked	6 September 2013

Note: *Please send the original Policy with both signatures on it to the Norfolk CPU for the audit trail.*

Index

1. Introduction.......3
2. Purpose.......3
3. Business Continuity and Business Continuity Management (BCM).......3
4. Business Continuity Management Process.......4
5. Objectives.......4
6. Critical Core Police Functions.......4
7. Business Impact Analysis.......5
8. Plans.......6
9. Invocation of Plans (flow chart available at Appendix B).......8
10. Post-Event Actions.......9
11. Embedding of Business Continuity Management.......9
12. Training, Exercises and Reviews.......10
13. Security of Plans.......10
14. Storage/Availability of Plans.......10
15. Roles and Responsibilities.......10
16. Appendix A – Business Continuity Management Process – flowchart.......11
17. Appendix B – Invocation of Plans – flowchart.......13

Legal Basis

Legislation specific to the subject of this policy document

Section	*Act (title and year)*
	Civil Contingencies Act (CCA) 2004

Other legislation which you must check this document against (required by law)

Act (title and year)
Human Rights Act 1998 (in particular A.14 – Prohibition of discrimination)
Equality Act 2010
Crime and Disorder Act 1998
Health and Safety at Work etc. Act 1974 and associated Regulations
General Data Protection Regulation (GDPR) and Data Protection Act 2018
Freedom Of Information Act 2000
The Civil Contingencies Act 2004

Other Related Documents

- Business Continuity Management - Emergency Preparedness (Home Office 2012)
- International Standard for Business Continuity ISO 22301

1. Introduction

1.1 The Civil Contingencies Act (CCA) 2004 places a duty on the police, as a Category 1 responder, to produce business continuity plans to ensure they can continue to carry out their civil protection functions and maintain critical services in the event of an emergency.

1.2 This policy is based on standards defined by the Civil Contingencies Act 2004, Chapter 6 Business Continuity Management Emergency Preparedness (Cabinet Office March 2012), and the International Standard for Business Continuity ISO 22301.

1.3 Implementation of this policy is the responsibility of Policing Commanders and Departmental Heads. It applies to all police personnel, including Special Constables and may also affect stakeholders, suppliers and contractors.

1.4 The procurement process for business critical service contracts will include an assessment of the contractors' own business continuity arrangements to ensure contractors are able to deliver an acceptable level of service in the event of their own operations being compromised.

1.5 Business Continuity plans must be completed by all departments/units that directly or indirectly support the delivery of Norfolk and Suffolk constabularies core functions.

1.6 Specific roles and responsibilities are identified at the end of this document.

2. Purpose

2.1 The purpose of this policy is to ensure that in the event of any disruption of service, critical core police functions continue to be performed to an acceptable level of service and recovery from disruption is both timely and effective.

3. Business Continuity and Business Continuity Management (BCM)

3.1 Business continuity is the strategic and tactical capability of the organisation to plan for and respond to incidents and business disruption in order to continue business operations at an acceptable predefined level.

3.2 Business continuity management provides the strategic framework for improving an organisation's resilience to interruption. Its purpose is to facilitate the recovery of key business systems and processes within agreed time frames, while maintaining the delivery of Category 1 responder's identified critical core functions. It assists organisations to anticipate, prepare for, prevent, respond and recover from disruptions, whatever their source and whatever aspect of the business they affect.

3.3 It is important not to confuse Business Continuity Management with operational response to major incidents. Business continuity management focuses on internal issues to maintain organisational abilities whereas response to major incidents focuses on external events.

4. Business Continuity Management Process

4.1 Business Continuity is based upon the ISO business life cycle “Plan-Do-Check-Act” model.

4.2 The model recommends a series of actions which will assist in an effective BCM management programme.

4.3 For a summary of the “Plan-Do-Check-Act” model - see appendix A.

5. Objectives

5.1 The primary objective is to manage business disruptions in a way that reduces impact on the organisation to an agreed acceptable level. To achieve this, both Norfolk and Suffolk Constabularies will:

- Manage any crisis arising from serious disruption to our business continuity and the consequence of any such crisis.
- Ensure continuation of critical core functions.
- Manage a return to ‘normality’.
- Identify lessons learnt from any disruption and/or exercise.
- Protect image and reputation.
- Improve processes.
- Strengthen ability to deal with internal/external disruptions to our key services and critical activities.
- Raise business continuity awareness within the organisation.

6. Critical Core Police Functions

6.1 The following core functions have been identified as critical - those which must be maintained/restored in the event of a serious disruptive event:

- Maintaining a system of command, control and communication - (for example answering 999 calls, Contact and Control Room (CCR), deploying to Grade 'A' calls, etc).
- Saving life, securing public safety and maintenance of public order (for example mobile patrols, visible presence).
- Containing an emergency, preventing escalation or spread.
- Dealing with prisoners and supporting the Custody / Criminal Justice Process.
- Dealing with major or critical incidents - investigating and detecting crime.

- Protecting the health, safety and welfare of staff.
- Assisting other agencies in response and recovery operations.

6.2 Activities that service the above critical core functions are identified through the Business Impact Analysis process – see below.

7. Business Impact Analysis

7.1 All Business Continuity Plans must be based on a Business Impact Analysis (BIA). Business Impact Analysis is the process of analysing business activities and the affect that a business disruption might have upon them. The process requires all activities to be prioritised based on a threat and risk assessment. Each critical activity identified in this process requires a recovery time to be set and resources and interdependencies to be recorded.

7.2 A business impact assessment template is available from the Business Continuity Manager to assist in the collection of information required for the business continuity plan. When complete, the template should be kept with the business continuity plan as supporting documentation.

7.3 All police personnel are advised to be familiar with the National Decision Model and to use the model, as appropriate, throughout the business impact analysis and recovery process.

7.4 Each of the following areas must be examined prior to compiling a business continuity plan:

Identify Critical Activities

7.5 These are the key activities that contribute to the achievement of one or more of the critical core functions listed in Section 6.

Determine Impact of Disruption

7.6 The impact of disruption for each critical activity should be considered in terms of the ability to deliver core critical functions, and the impact on stakeholders. The maximum tolerable period of disruption (MTPD) should be established and the minimum staffing levels required to maintain the activity.

Risk Assessment

7.7 The risk assessment process identifies risks, the level of impact and the likelihood that the risk will occur. The following areas should be considered when carrying out a risk assessment:

- Premises
- IT/Communications
- People/Staff

- Third Party Suppliers

7.7 For guidance on risk assessment, please see joint policy ‘Risk Management’ available on both forces intranet sites, or contact the Risk Management Team.

Senior Management Team Strategy

7.8 Based on the risk assessment, the Senior Management Team considers the activities and risks identified and will decide whether or not to agree the proposed approach/strategy to protect the critical activities.

Recovery and Resource Profile

7.9 In line with the Senior Management Team Strategy, the maximum tolerable period of disruption (MTPD) must be identified by ascertaining the:

- Maximum time period after the start of the disruption within which each activity needs to be resumed;
- Minimum level at which each activity needs to be performed upon resumption;
- Length of time within which normal levels of operations need to be resumed; and
- Resources that will be required to achieve this.

7.10 Further information is available from the Business Continuity Manager.

8. Plans

Business Continuity Plan (Silver)

8.1 Local Policing Commands (LPCs) / Departments that deliver critical activities, are required to compile their own business continuity plans under guidance from the Business Continuity Manager. They are responsible for identifying potential risks and vulnerabilities that may exist, assessing those risks and identifying a planned response to potential critical activity disruption.

8.2 Silver plans are written to an agreed established template available from the Business Continuity Manager.

8.3 Each LPC/Department must have a Business Continuity Lead (BCL) nominated by the Local Policing Commander/Departmental Head. That person will be the single point of contact with support from the Business Continuity Manager.

8.4 In addition, there will be a Plan Owner for each LPC/Department. The plan owner will be responsible for ensuring that their Silver Plan is published on time, updated where necessary and validated within a planned exercise schedule. The Business Continuity Lead and Plan Owner for a LPC/Department can be the same person. Training will be provided to the BCLs and Plan Owners by the Business Continuity Manager.

8.5 Once the Silver Plans are created they need to be approved by the plan owners' Policing Commander/Departmental Head. Once signed-off/approved they will be distributed via the Business Continuity Manager who will undertake corporate responsibility for their co-ordination and collation, as well as introducing a quality assurance element to the process.

8.6 Silver plans feed into the 'Gold' level Crisis Management Plan.

Crisis Management Plan (Gold)

8.7 A Crisis Management Plan is activated in the event of serious disruption (affects more than one business area) and a Crisis Management Team convened

8.8 The Crisis Management Plan is developed and owned by the Business Continuity Manager.

Loss of Premises Plan

8.9 Police premises identified by the Estates Department as Tier 1 or Tier 2 will have a "Loss of Premises plan". The owner of these plans will be the Estates Department; however, the plans will be retained and updated by nominated staff at the premises for their use/reference.

8.10 Norfolk Constabulary and Suffolk Constabulary each have their own Estates strategy 2016-2020.

8.11 The strategy documents reflect in particular the actual and forecast police funding reductions in current and future years and the need to make savings and achieve best value-for-money by downsizing the estate wherever possible and practical and making best use of existing and future assets.

8.12 Where either Constabulary are utilising PFI buildings there are agreed time frames between the PFI provider and the constabularies. For the Police Investigation Centres - within 20 days of an event / claim the PFI Provider must provide a reinstatement plan to repair and reinstate or replace any assets affected. For the Norfolk Command and Control Room the Constabulary will provide written notice to the PFI Provider within 10 working days of the event. The PFI contract allows for the parties to meet and for the PFI Provider to prepare a reinstatement plan to repair and reinstate or replace any assets affected. The PFI Provider must complete the plan within a maximum time frame of 6 months from the original event date.

Third Party Suppliers

8.13 Where any critical core functions are reliant on third party suppliers, Procurement and Supplies (Norfolk and Suffolk) will grade those contracts as ‘high risk’ to the Constabularies. Any tender process should ensure that third party suppliers have the necessary business continuity plans in place.

8.14 Departmental business owners will need to ensure they advise Procurement and Supplies (Norfolk and Suffolk) of the business continuity measures they require being in place. Example definitions of potential ‘high risk’ areas are provided on the Contract Planning and Control Document.

9. Invocation of Plans (flow chart available at Appendix B)

9.1 The individual who discovers or receives information about a situation that could result in a critical disruption during office hours, should notify the Plan Owner, the Business Continuity Manager and relevant CCR Inspector (contact details available in the Business Continuity Plan). If out of office hours, the on-call Superintendent should be contacted via CCR Inspector.

9.2 The trigger for invocation of the plan(s) will be an event which causes one or more of the following:

- Total or partial loss of any workplace;
- Total or partial loss of any electrical power / computer systems / telephony;
- Total or partial loss of personnel;
- Significant interruption to supplies (e.g. fuel for vehicles / generators).

9.3 When one or a combination of events occurs, which results in one or more of the consequences outlined above, the Local Policing Commander/Departmental Head, will decide whether or not to activate their Silver plan. Upon activation of the plan, the plan owner will immediately convene its Continuity Recovery Team (CRT).

9.4 In addition, the Local Policing Commander/Departmental Head, when deciding upon activation, will assess the disruption of the event and its impact or likely impact on other business continuity plan owners. Where it is apparent that the disruption will impact on other plan owners, they will notify the relevant Recovery Manager (DCC) and the Head of

Operational Planning, Joint Specialist Operations Department, as soon as practicable.

9.5 The Recovery Manager will take command, invocate the Gold Plan and activate a Crisis Management Team (CMT) who will provide strategic co-ordination for the actions of the silver plan owners.

9.6 Where the disruption can be contained within the business area with little or no impact on other plan owners, the disruption will be managed by the LPC/Department’s own CRT.

10. Post-Event Actions

10.1 On conclusion of the invocation of a Plan, and the return to normality, the Business Continuity Lead/Plan Owner will ensure that all personnel and internal/external partners are informed.

They will also:

- Conduct an internal investigation into the cause;
- Identify lessons learned via staff debriefing;
- Review and update the Plan (updated plans should be forwarded to the Business Continuity Manager);
- Send concluding report within 28 days of the resolution of the event to the Business Continuity Manager.

11. Embedding of Business Continuity Management

11.1 All staff, police officers and volunteers have a role to play in the effective embedding of Business Continuity Management into the culture of both Norfolk and Suffolk Constabularies.

11.2 When new initiatives are in the planning stage early consultation with the Business Continuity Manager is essential to ensure business continuity is considered and built into the project/development.

11.3 The Business Continuity Manager will give an overview of Business Continuity Management at newly promoted sergeants and supervisors courses.

11.4 Policing Commanders/Departmental Heads should seek to develop a business continuity management culture by:

- Giving proactive support to the BCM process;
- Encouraging training and awareness in BCM;
- Ensuring ownership of BCM;
- Demonstrating a commitment to the programme of maintenance, review and testing of the BCM plans;
- Communicating the importance of BCM to all staff and their roles and responsibilities; and

- Including a Business Continuity standing item on Command Team meeting agenda.

12. Training, Exercises and Reviews

12.1 Training will be provided to Business Continuity Leads and Plan Owners by the Business Continuity Manager.

12.2 It is the responsibility of Policing Commanders/Departmental Heads to notify the Business Continuity Manager of newly appointed Business Continuity Leads/Plan Owners.

12.3 Business Continuity Plans are to be exercised and reviewed at least annually in order to validate them. Plans will be exercised during June/July and reviewed in November/December. Each Plan Owner is responsible for exercising and reviewing their plan, under the guidance of the Business Continuity Manager.

12.4 Any amendments to Silver or Loss of Premises Plans will be sent to the Business Continuity Manager in order for the master (electronic) copy to be updated.

13. Security of Plans

13.1 The content of Loss of Premises, Silver and Gold plans provide a comprehensive overview of the police response to a serious disruptive event and would allow unauthorised persons to plan a course of action that could place police personnel and the public at risk. Therefore, the plans are protectively marked as 'OFFICIAL SENSITIVE' and should not be released into the public domain.

14. Storage/Availability of Plans

14.1 Each Plan Owner will store a hard copy and electronic copy of their own plans. They must ensure the most up-to-date version is available and old versions destroyed.

14.2 A copy of all plans will be kept by the respective CCR to enable access out of office hours.

14.3 The master electronic copy of all plans will be retained by the Business Continuity Manager, Joint Specialist Operations Department.

15. Roles and Responsibilities

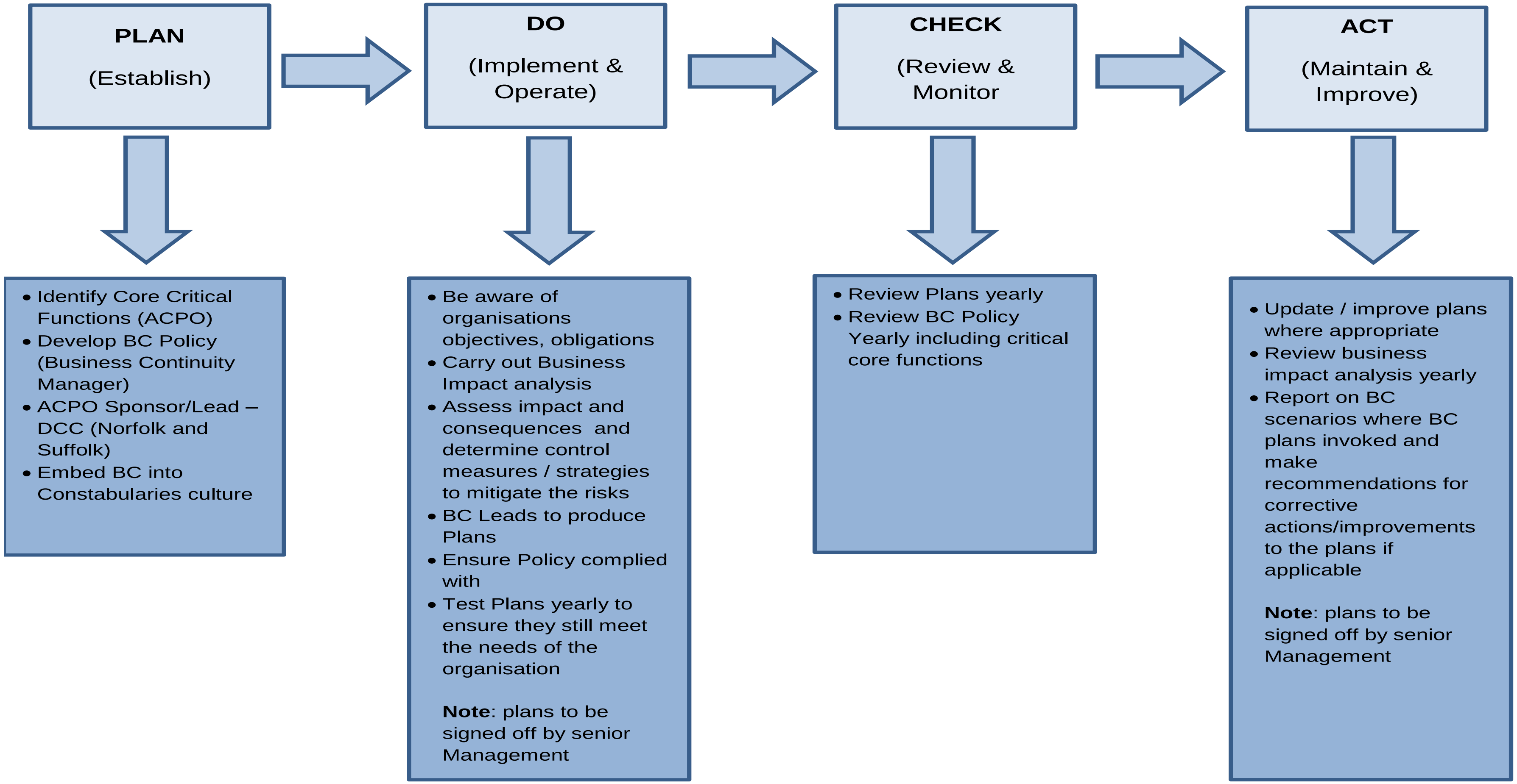
Role Title	Responsibilities
Respective DCC (Norfolk/Suffolk)	• Make sure that service areas respond accordingly to the requirements of the process. • Ensure there is a consistency to high-level

Recovery Manager (DCC)	decision making, if required. • Command of Gold Crisis Management Team
Business Continuity Manager	• Work with Plan Owners to ensure plans are in place. • Monitor and benchmark the testing of business continuity plans on an annual basis. • Provide training and professional advice to support the development, implementation and testing of business continuity plans. • Be responsible for ensuring that any lessons learned from testing or activation of any business continuity plans are shared with other Business Continuity Leads and Plan Owners.
Policing Commanders/ Departmental Heads	• Identify Business Continuity Lead/Plan Owner. • Notify Business Continuity Manager of new Business Continuity Leads/Plan Owners.
Plan Owner	• Conduct Business Impact Analysis • Produce effective business continuity plans. • Ensure business continuity plans are available to support the delivery of core policing functions during a disruption.
Business Continuity Leads	• Review business continuity plans at least annually. • Exercise and evaluate business continuity plan(s) at least once a year, amending as required.
Risk Management	• Assist Business Continuity Lead/Plan Owner with Business Impact Analysis. • Liaise with Insurers.

16. Appendix A – Business Continuity Management Process – flowchart

Appendix A

BUSINESS CONTINUITY MANAGEMENT PROCESS



PLAN

(Establish)

- Identify Core Critical Functions (ACPO)
- Develop BC Policy (Business Continuity Manager)
- ACPO Sponsor/Lead – DCC (Norfolk and Suffolk)
- Embed BC into Constabularies culture

DO

(Implement & Operate)

- Be aware of organisations objectives, obligations
- Carry out Business Impact analysis
- Assess impact and consequences and determine control measures / strategies to mitigate the risks
- BC Leads to produce Plans
- Ensure Policy complied with
- Test Plans yearly to ensure they still meet the needs of the organisation

Note: plans to be signed off by senior Management

CHECK

(Review & Monitor

- Review Plans yearly
- Review BC Policy Yearly including critical core functions

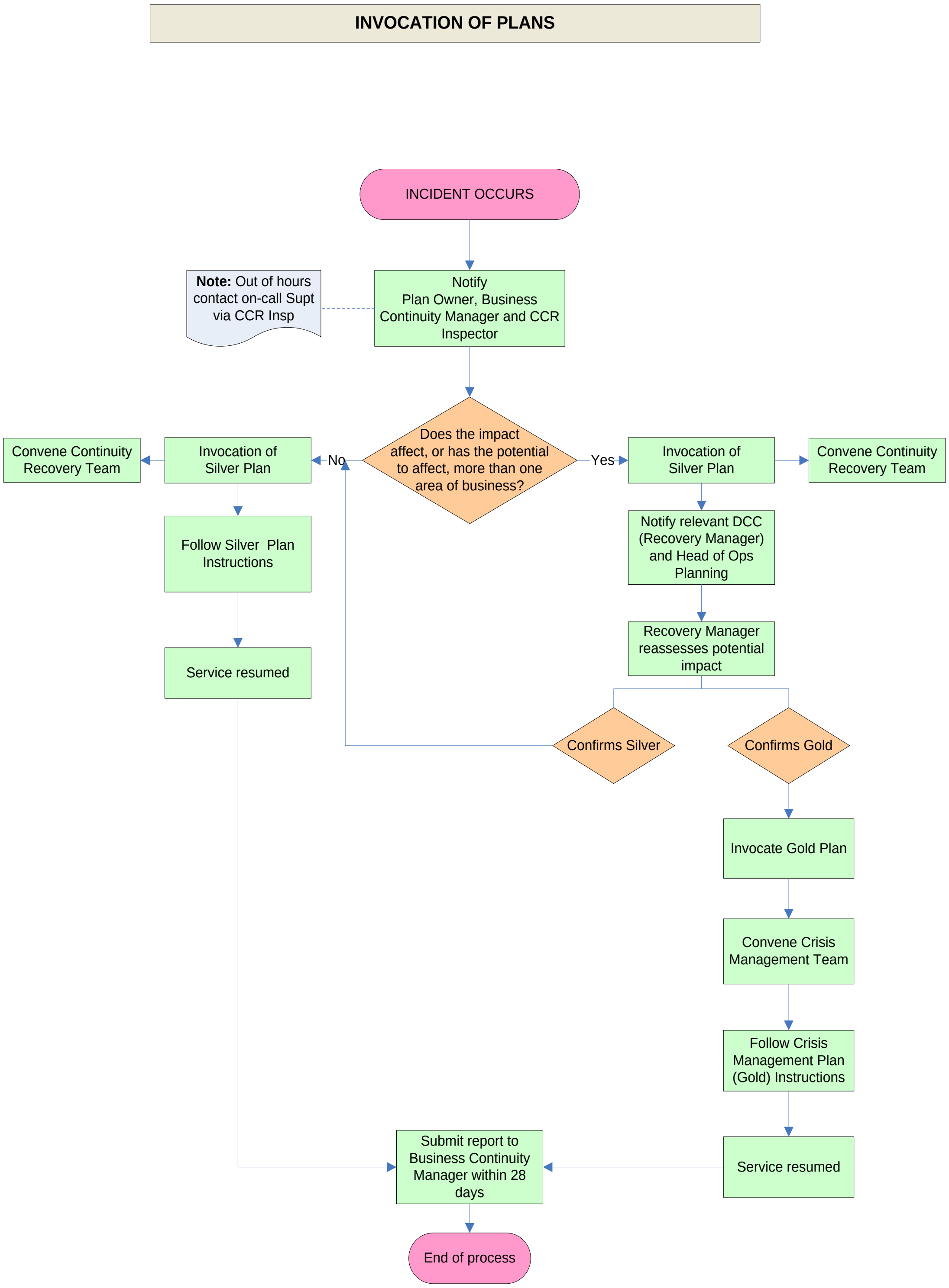
ACT

(Maintain & Improve)

- Update / improve plans where appropriate
- Review business impact analysis yearly
- Report on BC scenarios where BC plans invoked and make recommendations for corrective actions/improvements to the plans if applicable

Note: plans to be signed off by senior Management

17. Appendix B – Invocation of Plans – flowchart


INVOCATION OF PLANS
INCIDENT OCCURS
Note: Out of hours contact on-call Supt via CCR Insp
Notify Plan Owner, Business Continuity Manager and CCR Inspector
Does the impact affect, or has the potential to affect, more than one area of business?
No
Yes
Invocation of Silver Plan
Convene Continuity Recovery Team
Follow Silver Plan Instructions
Service resumed
Invocation of Silver Plan
Convene Continuity Recovery Team
Notify relevant DCC (Recovery Manager) and Head of Ops Planning
Recovery Manager reassesses potential impact
Confirms Silver
Confirms Gold
Invocate Gold Plan
Convene Crisis Management Team
Follow Crisis Management Plan (Gold) Instructions
Service resumed
Submit report to Business Continuity Manager within 28 days
End of process