THE CHIEF CONSTABLE OF CLEVELAND

Business Continuity Planning

Internal audit report 1.20/21

Final

14 August 2020

1. EXECUTIVE SUMMARY

With the use of secure portals for the transfer of information, and through electronic communication means, remote working has meant that we have been able to complete our audit / assignment and provide you with the assurances you require. It is these exceptional circumstances which mean that 100 per cent of our audit has been conducted remotely. Based on the information provided by you, we have been able to sample test.

Why we completed this audit

An audit was undertaken as part of the 2020/21 internal audit plan to assess the effectiveness of the Force's Business Continuity Plans (BCPs) and whether they are understood to ensure that the service delivery can be continued in the event of an incident or crisis.

The Force operates 35 departmental and/or unit BCPs, which are designed to cover all critical areas of business operations, these critical functions were initially identified as part of a business impact assessment, conducted by the Business Continuity Champion (BCC) and overseen by the Business Continuity Manager (BCM). Each plan has a BCC and overarching plan owner. The BCC is responsible for liaising with their units and the BCM, who together update and amend their plans to reflect existing practises, functions, contingency measures and changes to key personnel.

The BCM is responsible for the wider business continuity framework including designing and undertaking of plan testing, reviewing and approving on an annual basis, and raising general awareness amongst BCCs and other key personnel.

As part of this review, we spoke with the BCCs for a sample of unit BCPs. The departments interviewed as part of the review were:

- Covert Standards;
- Custody;
- Training and Organisational Development;
- Special Branch; and
- Organised Crime.

Instead, it was geared towards considering the risks posed to each function, on a departmental basis. While the reported cases of Covid-19 (the Coronavirus) were increasing throughout the UK at the time of audit testing (May 2020), this review does not focus solely on the BC arrangements in the event of a pandemic. Rather, the audit was geared towards considering the risks posed to each function on a departmental basis and focused particularly on the Force's administrational approach and operational planning in place to mitigate the risks posed by a BC issue. The review has therefore not provided assurance on the Force's response to individual BC incidents, including Covid-19.

Conclusion

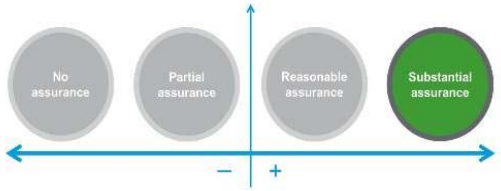
Through testing conducted as part of this review, we found that the control framework relating to business continuity planning was well-designed, operating effectively and being applied consistently; however, we did identify isolated incident of deviations from the control framework as well as areas where the Force can strengthen their existing framework. As a result, we have agreed **one medium** and **three low** priority management actions.

The Business Continuity Manager role was established in 2008 as a dedicated resource to drive the business continuity arrangements of the Force. The Strategic Finance Manager and the Chief Constable's Chief Finance Officer also engage actively in the Force's business continuity framework.

As the actions raised were considered isolated incidents or concerned the enhancement of existing controls, we have concluded that the Chief Constable of Cleveland can take substantial assurance regarding the integrity of the control environment surrounding BC planning at the Force.

Internal audit opinion:

Taking account of the issues identified, the Chief Constable of Cleveland can take **substantial assurance** that the controls upon which the organisation relies to manage the identified area are suitably designed, consistently applied and operating effectively.



Key findings

We identified the following well-designed controls that had been applied consistently:

The Force has service continuity guidance in place outlining the framework to adhere to. Testing found practices were in line with this guidance.

Each BCP has a BCC assigned, who was continually liaising with their respective units for any updates, including cascading any pertinent information to key personnel detailed within the BCP.

Each plan is written as a standard operating procedure, including key facets such as key objections, critical functions and associated contingency controls/ measures and activation and recovery teams.

Testing found that the key risks associated with each unit had been readily identified and assessed within the plan, this included mapping a series of recovery or contingency steps that would be implemented to respond to a continuity incident issue such as loss of premise or power outage.

We found the review mechanisms to be robust, adequate and had been undertaken within a timely manner for the sample of BCPs sampled. Reviews included desktop review and face to face meetings.

We found the availability of plans to be suitable, including access restricted on SharePoint, within the Control Room for out of hours activation as well as confirming that each BCC had established suitable BCP off-site measures.

A service continuity update was provided to the Joint Audit Committee on a half yearly basis.

However, we identified the following issues that have resulted in the agreement of one medium priority action:

Testing identified that two of the five BCPs sampled had not been subject to either a live-test or simulated tabletop test exercise, designed by the BCM. However, we were advised that due to capacity issues and the units selected being identified as ‘low vulnerability’, this had resulted in no testing being conducted since the BCPs inception. We did acknowledge the BCMs awareness of this, and their intention to remedy this with a testing programme for all BCPs.

Further to this, we have identified a further **three low** priority actions, detailed of which can be found in section two of this report.

2. DETAILED FINDINGS AND ACTIONS

This report has been prepared by exception. Therefore, we have included in this section, only those areas of weakness in control or examples of lapses in control identified from our testing and not the outcome of all internal audit testing undertaken.

Area: Business Impact Assessments				
Control	Each unit has undertaken a Business Impact Assessment (BIA) that identifies key critical functions that must be restored or continued to deliver the Units core activities. The assessment requires the BC Champion to identify both their critical functions and a series of controls or contingencies which will be used to mitigate the total or partial loss of an identified function.		**Assessment:** **Design** ✓ **Compliance** ×	
Findings / Implications	On review of each BIA, we confirmed that the core functions as identified by the BC Champions (at that time) had been reflected within the current BC Plans. It was identified that the BIAs had been conducted between October 2017 and September 2018. Discussions with the BC Manager established that as opposed to undertaking a BIA each year, the decision had been taken to reinforce the review controls (as detailed below) to ensure each unit is subject to adequate scrutiny in order to identify any changes that may affect the delivery of any of its core functions. This included both changes in systems, significant changes in personnel or single points of failure. However, it was acknowledged through a meeting with the BC Manager that where a significant change in a department's environment does occur or the department operations have evolved since the previous review, the unit may benefit from performing another BIA and amending any risk scoring in light of the changes. Without re-performing impact assessments, there is a risk that new priorities are assessed, leading to misaligned priorities within continuity plans. We reviewed each of the BIA for the chosen units and found that in most instances the inherent risk scores had been reduced (where possible) by mitigating controls or contingency measures. However, within two plans for the Economic Crime Unit and the Training and Organisational Development Unit's BIA, we identified four instances where the controls and contingency measures showed no effect on the residual risk score. Without establish mitigating controls that reduce the residual risk, there is risk that redundant controls are established, leading to ineffective use of resources.			
Management Action 1	Where either the BC Manager or Champion identify significant changes that materially affect the critical function or activities of the BC Plan, a revised Business Impact Assessment will be undertaken and the findings updated within the Business Continuity Plan. This will be built into the annual business continuity meeting, where required.	**Responsible Owner:** Business Continuity Manager	**Date:** August 2020	**Priority:** Low

Area: Business Impact Assessments	
	The BC Champion will review the risk scores identified and assess whether the existing contingency measures / controls are appropriate and whether additional measures need to be established.

Area: Key contacts and activation lists			
Control	Operational BC Plans are developed to address the key threats posed to the critical functions of a service area. Each critical function includes suitable contingency arrangements and relevant contact numbers. Plans also cover a broad range of scenarios which may pose issues to business continuity.	**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	Each BC Plan outlines their critical functions that are required in order to deliver the minimum service requirements. Underpinning each of these critical functions were a series of contingency arrangements each tailored to how departments would maintain service delivery, before the Recovery Management Team would seek to re-establish critical functions in line with the stated recovery time objectives. On review of the contingency measures for each of the BC Plans, we considered them suitable to the circumstances. For a sample of 20 contacts tested across the five sampled BC plans, we verified 18 contact details; however, we found two direct or extension numbers that were currently outdated. Without having updated contact numbers, there is a risk that activation of the elements of the plan are delayed, causing increased risk to staff or re-establishing business continuity. We held discussions with five BC Champions to identify whether key risk rising from their departmental operations are being addressed. **Economic Crime Unit (ECU)** The ECU, comprised of the Economic Crime, Cyber Crime and Paedophile Online Investigation Teams (POLIT) are responsible for investigation of child grooming, high value fraud cases, online paedophile suspects, cybercrime as well as confiscation of cash / seizure and action fraud research amongst other areas. The greatest risks identified by the BC Champion was shortage of specialist staff / teams and access to covert systems used to receive referrals, indecent images and identify potential suspects.		

For team related risk, the BC Plan had identified a number of contingencies including sourcing trained staff from neighbouring forces and cross-skilled officers. Access to systems can be done remotely or through other neighbouring forces, where a system is down contingencies allow for Compact Disc (CD) access to images or referrals within a secure environment.

Special Branch (SB)

SB is responsible for receiving, assessing and disseminating information and intelligence of threats to national security from terrorism and violent extremism. The main risk posed to the department is shortage of staff and surge periods that may increase workloads, both these factors had been planned for by using collaborative agreements with other regional forces such as Durham and North Yorkshire, and other regional counter terrorism organisations.

The BC Champion informed us that since a lot of contingencies were reliant on other forces and organisations, they would confirm the arrangements with their BC counterpart at other forces, following each BC plan review.

Training and Organisational Development

The Training and Organisational Development department is used primarily to deliver training and staff development through e-learning, learning programmes and face-to-face training. The BC Champion explained that the main risk posted to their unit is housing of staff training and the use of equipment for on-site training sessions, which can be classroom or gymnasium (or equivalent) based.

In regard to alternate locations and equipment, agreements were in place with Cleveland Fire Service, Durham and North Yorkshire for smaller training sessions, and for larger sessions an agreement was in place with the Territorial Army in Norton. The contingency arrangements had also considered the use of alternate rooms within the main premises.

Organised Crime

The Organised Crime Unit is deployed to tackle serious and organised crime, including providing specialist advice in serious crimes, and maintaining surveillance capability. The key business continuity risks identified by the BC champion were access and availability of specialist equipment, vehicles and staff.

To mitigate these risks, we identified that the BC Plan had established relations with the North East Regional Special Operations Unit (NERSOU), who would be able to provide back-up vehicles, equipment and staff. NERSOU would also act as a contingency measure, should the Cleveland base be unusable.

Covert Standards

Area: Key contacts and activation lists				
	The Covert Standards primary purpose is to provide fully trained Authorised Officers to facilitate two pieces of investigative legislation. The BC Champion had identified two primary risks in relation to their unit, those being the shortage of Authorised Officers and the use of covert communication systems. To mitigate these risks, we identified that the unit had a collaborative agreement with both Durham and Northumbria Authorising Officer function, with support from other regional Authorising Officers if necessary. For the communication systems, it was stated that these servers are maintained off-site and the unit can rely upon the collaborative agreement with Durham and Northumbria if required. For each of the BCP, we identified that a series of generic scenarios were stated, and each plan detailed how the unit would respond to loss of key staff, communications, working site or rooms, equipment including specialist equipment, utilities, IT and vehicles. We noted that for the incidents that required evacuations the plans had also detailed the location, security and equipment considerations. Furthermore, there were contingencies listed for specialist equipment, IT systems and vehicles alongside suitable recovery time objectives.			
Management Action 2	The BC Manager and/or BC Champion will review the outdated contacts identified and either update or remove these.	**Responsible Owner:** Business Continuity Manager	**Date:** September 2020	**Priority:** Low

Area: Business Continuity Plan Testing			
Control	Thematic tabletop exercises are conducted by the BC Manager three to four times a year. These centre around a series of scenarios that concern business continuity, and BC Champions and their team / key personnel are required to activate their plans in a testing simulation. A report is produced post-exercise listing any recommendations or identified action areas. Action areas are followed up in conjunction with the BC Champion and BC Manager reviews.	**Assessment:** **Design** **Compliance**	 ✓ ×
Findings / Implications	**Economic Crime Unit (ECU)** We identified that 'Exercise Minister' was undertaken in October 2019. This table-top exercise developed by the BC Manager, provided a scenario that assessed the ability for the ECU and Cyber Crime Unit to adopt to contingences with a loss of their staff, IT and office location, whilst dealing with normal requests for service. On review of the report, we considered the scenario as robust, integrating test scenarios that tested different facets of their BC Plan. We noted that this exercise did not involve the Paedophile Online Investigation Team (POLIT) who are also part of the wider ECU.		

As part of the outcome report, there had been a series of recommendations raised, namely the availability of the BC Plan to the wider department, off-site 'grab bags' and referencing other external supported units. In each instance we tracked these through the existing BC Plan, and found recommendations had been reflected, where appropriate.

Training and Organisational Development

We identified that the Training and Organisational Development Unit had been subject to a real-life testing of their BC Plan in March 2019, which involved a structural issue that caused the classrooms being made unusable on the ground and first floor. A further real-life scenario had also taken place in 2018 regarding a power outage that affected trainer's workplace. The outcome of this incident was reflected within the existing BC Plan, by allowing agile working for trainers as well as multiple contingency work locations. In regard to the structural issue in 2019, we confirmed that shortly following the incident the BC Manager in conjunction with the Learning and Development Manager had met as part of a Gold Group to discuss the long-term impact as well as ongoing issues that needed to be resolved to ensure training and development needs could continue.

The outcome of this incident was to create a separate Training and Organisational Development Business Continuity Plan which considered these types of incidents, amongst others. We have not raised a concern here as we considered the formation of the Gold Group as an effective means to mobilise resources to continue business, as well as identifying that the group had considered 'continuity' issues. This is exemplified in the formation of the separate Training and Organisational Development Business Continuity Plan.

Covert Standards, Organised Crime and Special Branch

We identified that the Organised Crime, Special Branch and Covert Standards Units had not been subject to a table-top testing exercise. Discussions with the Business Continuity Manager established that due to capacity issues three to four tests were currently being developed and run in-year. The BC Manager also explained that the results of the vulnerability exercise undertaken in 2018 had indicated these three units were considered as 'low vulnerability' for testing, when compared to the other 32 units. We obtained the BC exercise schedule and verified that the three units not subject to testing were identified as low vulnerability.

Despite this, we identified that without undertaking regular testing of BC plans, there is a risk that operational issues arise in real life scenario, leading to greater risk of business disruption. Furthermore, we acknowledged that going forward the BC Manager was planning to develop a testing programme, which would aim to test all units that have not been previously tested. We were advised that the testing programme would be driven on two factors, whether the unit was considered 'vulnerable' as per the exercise described above, and whether the unit's critical functions were considered critical in terms of Force function delivery i.e. integral to operating as an effective police force. This information has been reflected within the finding.

Management Action 3	The BC Manager will develop a testing programme with a schedule of one testing exercise per month (subject to COVID-19 restrictions being lifted). This will include tabletop BC scenario testing for the Covert Standards, Organised Crime and Special Branch and POLIT Units.	**Responsible Owner:** Business Continuity Manager	**Date:** October 2020	**Priority:** Medium

Area: Business Continuity Refresher and Awareness sessions			
Control	Two refresher business continuity briefings were delivered by the BC Manager to BC Champions. This meeting reviewed incidents, emerging trends and lessons learnt from past testing and plan development.	**Assessment:**	
		Design	✓
		Compliance	×
Findings / Implications	We identified that two business continuity briefings had been undertaken in 2019, one held in September and the other in November. The BC briefing provided a refresher on importance of business continuity including emerging trends, single points of failure, utilising the control room and plan management. The meeting also provided an opportunity to provide any cross-unit feedback or findings. Through review of the attendee list we identified that four of the five of the BC Champions within our sample had attended the briefing, and in total 33 of 35 BC Champions or representatives, had attended one of the briefings; however, we identified that the BC Champion for Special Branch (included in our sample) had not attended either briefing. We did acknowledge that the BC Champion for Special Branch had attended a similar BC briefing in 2017. Due to both these factors listed above, we considered this issue to be an isolated incident. Without attending briefings there is a risk that pertinent information is missed and not considered in BC plans, leading to gaps in business continuity responses or coverage.		
Management Action 4	Where BC briefing or sessions are held the BC Champion will endeavour to attend. Where this is not possible, they will send either their BC Deputy or another representative.	**Responsible Owner:** Business Continuity Manager	**Date:** December 2020	**Priority:** Low

APPENDIX B: CATEGORISATION OF FINDINGS

Categorisation of internal audit findings	
Priority	**Definition**
Low	There is scope for enhancing control or improving efficiency and quality.
Medium	Timely management attention is necessary. This is an internal control risk management issue that could lead to: Financial losses which could affect the effective function of a department, loss of controls or process being audited or possible reputational damage, negative publicity in local or regional media.
High	Immediate management attention is necessary. This is a serious internal control or risk management issue that may lead to: Substantial losses, violation of corporate strategies, policies or values, reputational damage, negative publicity in national or international media or adverse regulatory impact, such as loss of operating licences or material fines.

The following table highlights the number and categories of management actions made as a result of this audit.

Area	Control design not effective*		Non Compliance with controls*		Agreed actions		
					Low	Medium	High
Business Continuity Planning	0	(11)	4	(11)	3	1	0
Total					**3**	**1**	**0**

* Shows the number of controls not adequately designed or not complied with. The number in brackets represents the total number of controls reviewed in this area.

APPENDIX C: SCOPE

The scope below is a copy of the original document issued.

Scope of the review

The internal audit assignment has been scoped to provide assurance on how the Chief Constable of Cleveland manages the following area:

Objective of the area under review
The organisation has adequate plans in place and they are understood to ensure that the service delivery can be continued in the event of an incident or crisis.

Scope of the review

To ensure the Force has business continuity plans within operational planning that are designed to provide effective advice to assist those responsible for a return to business as usual, within the most appropriate and planned timescales. As part of our review we will consider the following:

- Whether there is an operational business continuity policy and any associated procedures in place. This will include how these are communicated to relevant staff, are kept up to date and approved.
- The development of operational business continuity plans. We will assess the plans for completeness, and whether there are any key sections missing. We will interview a selection of business continuity owners as part of this process.
- Within the plans, an appropriate selection of arrangements are in place covering a broad range of scenarios. This will include review of how the scenarios covered within the plan are identified.
- The approval process for the operational business continuity plans.
- The responsibility for operational business continuity has been clearly assigned to key members of staff / officers.
- Regular reviews are undertaken to ensure that the plans in place remain up to date and fit for purpose.
- Access to business continuity plans are available off-site and reflect the most up to date version.
- Periodic business continuity tests are carried out.
- Results from tests are reviewed and action plans are developed where appropriate, to improve the processes based on areas of adverse performance.

- Whether there are any dedicated forums for operational business continuity. This will include review of whether regular updates are presented to senior management providing assurance that appropriate business continuity arrangements are in place.

The following limitations apply to the scope of our work:

- The review will not guarantee that in the event of an emergency the plan will ensure the stability of the operational infrastructure.
- We will not review the impact of Covid-19 or the Force's response to the pandemic.
- We will not provide assurance that actions identified within the plan are appropriate or that measures stated will actually assist in the objectives which the plan is set out to achieve.
- We will not guarantee that all appropriate individuals have read and reviewed plans in place and that staff fully understand the importance of business contingency planning.
- All testing will be compliance-based sample testing only.
- Our work will not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

Debrief held	28 May 2020
Draft report issued	11 June 2020
Responses received	14 August 2020
Final report issued	14 August 2020

Internal audit Contacts	Dan Harris, Head of Internal Audit
	Angela Ward, Senior Manager
	Philip Church, Client Manager
	Josh Martin, Senior Auditor
Client sponsor	Chief Finance Officer - Chief Constable
	Strategic Finance Manager
	Business Continuity Manager
Distribution	Chief Finance Officer - Chief Constable
	Strategic Finance Manager
	Business Continuity Manager

rsmuk.com

The matters raised in this report are only those which came to our attention during the course of our review and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Actions for improvements should be assessed by you for their full impact. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

Our report is prepared solely for the confidential use of **The Chief Constable of Cleveland**, and solely for the purposes set out herein. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from RSM Risk Assurance Services LLP for any purpose or in any context. Any third party which obtains access to this report or a copy and chooses to rely on it (or any part of it) will do so at its own risk. To the fullest extent permitted by law, RSM Risk Assurance Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to you on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

RSM Risk Assurance Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.