The Police and Crime Commissioner for Cleveland and the Chief Constable of Cleveland

Internal Audit Progress Report

2 October 2020

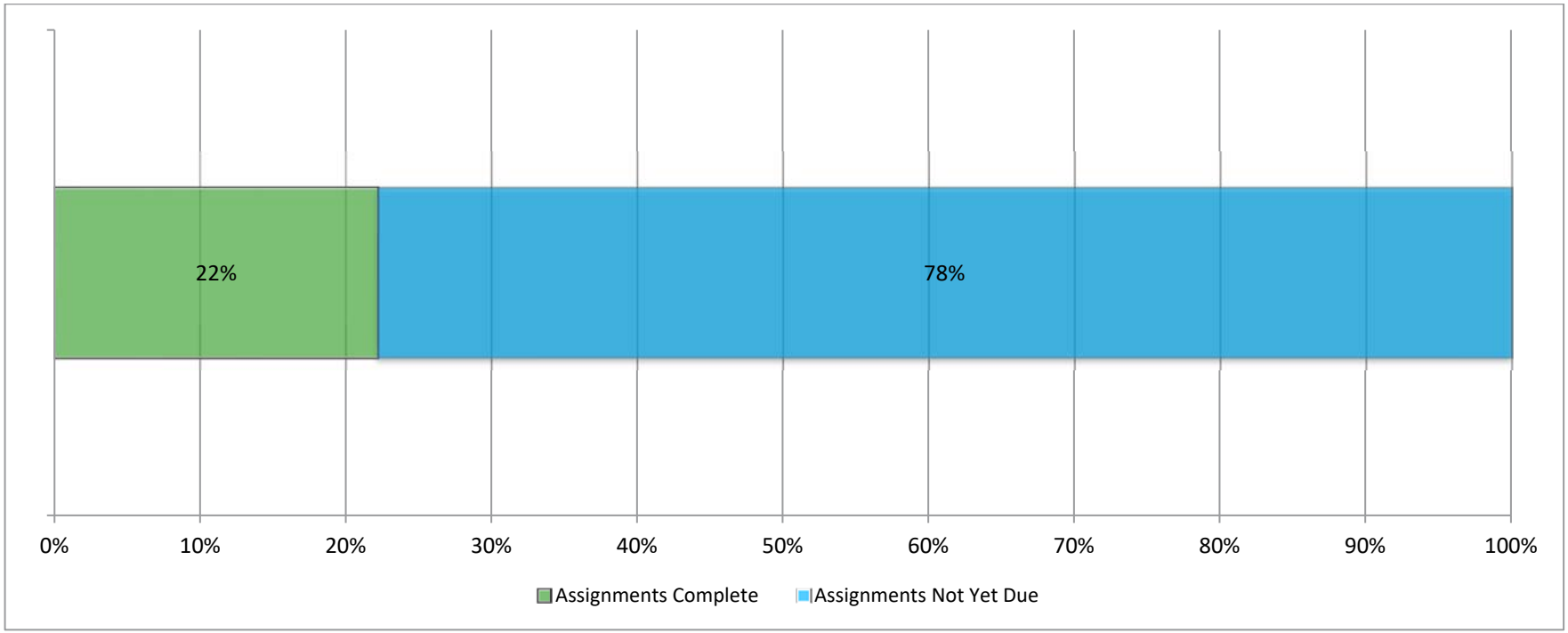
RSM

Contents

1 Introduction

The internal audit plan for 2020 / 2021 was approved by the Joint Audit Committee (JAC) on 29 June 2020.

The graphic below provides a summary update on progress against the 2020 / 2021 plan.



2 Reports

2.1 Summary of final reports being presented to this committee

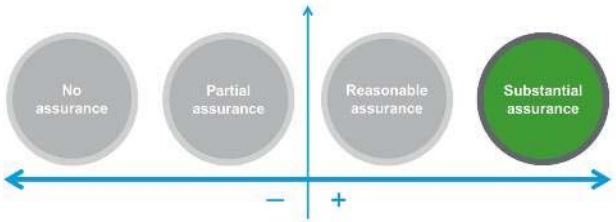
This section summarises the reports that have been finalised since the last meeting. We have finalised four reports since the previous meeting and these are detailed below:

Assignment	Actions agreed		
	L	M	H
Business Continuity Planning	3	1	0

Objective of the 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.

Overall assurance rating and management actions:



An overall assurance rating of **substantial assurance** has been given for this review. We have agreed **one medium** and **three low** priority management actions. The medium management action related to the development of tabletop exercises for Covert Standards, Organised Crime and Special Branch and POLIT Units.

Context:

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

Assignment	Actions agreed		
	L	M	H

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.

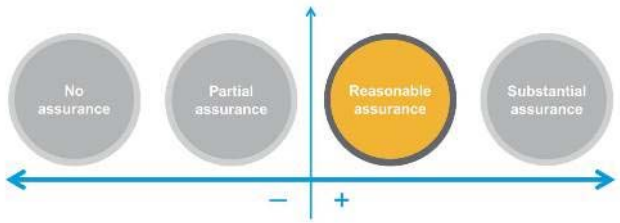
While the reported cases of Covid-19 (the Coronavirus) were increasing throughout the UK at the time of audit testing (May 2020), this review does not focus solely on the BC arrangements in the event of a pandemic. Rather, the audit was geared towards considering the risks posed to each function on a 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.

Assignment	Actions agreed		
	L	M	H
Risk Management	2	5	0

Objective of the review:

The organisations have an adequate and effective process in place to identify and manage both risks and opportunities that support the delivery of the Commissioner's Police and Crime Plan.

Overall assurance rating and management actions:



An overall assurance rating of **reasonable assurance** has been given for this review. We have agreed **five medium** and **two low** priority management actions. The medium management actions related to the following:

- At the time of review, we noted that the Baseline Risk Assessment had not been reviewed following the Force's recent PEEL Inspection.

- A listing of all current risk champions across the Force was obtained and reviewed. The listing contains a total of 25 departments and their corresponding risk champion. However, it was noted that a risk champion had not been documented for three departments (CDSOU, CID and Intelligence).

- Five risks were selected and tested from departmental risk registers. In two instances we confirmed that mitigating actions had been subject to regular review and had been maintained up to date. However, in the remaining three instances we noted that mitigating actions had surpassed their set review date. Instances were also noted where mitigating actions were vague and not clearly documented. Additionally, a large number of mitigating actions were found to have been documented which only resulted in a minor reduction to the relevant residual risk scores.

- The current seven documented risks within the 4risk software system for the PCC's strategic risk register were reviewed. In five instances we confirmed that mitigating actions had been subject to regular review and had been maintained up to date. However, in the remaining two instances it was noted that mitigating actions had surpassed their set review date.

Assignment	Actions agreed		
	L	M	H

- Instances were noted where assurance sources had not been documented against controls for risks within the Force's and PCC's strategic risk register as well as departmental risk registers.

Context:

The Force has a Risk and Insurance Manager in place who is responsible for the overall governance of the risk management process throughout the organisation. Heads of Department appoint risk champions from within the Management Team. Risk champions report directly to the Risk and Insurance Manager and are responsible for the day-to-day management of their departmental level risks. Risk champions meet with the Force's Risk and Insurance Manager on a quarterly basis to provide updates on existing departmental risks and discuss any new/emerging risks that may affect the relevant department. Departmental risks are also regularly reviewed at Senior Leadership Team (SLT) meetings.

The risks identified are recorded at either the strategic level, in a strategic risk register or at an operational level, in departmental risk registers. This two-tier approach ensures that the highest-level strategic risks, those which present the greatest challenge to the Force and PCC, are identified, evaluated and closely monitored. Risks are assessed and plotted on a 5x5 risk scoring matrix in line with their relevant impact and likelihood. Following the rating process, the subsequent score allocated to the risk will determine where the risk sits within the matrix and the level of attention the risk requires.

The four groups within the risk scoring matrix are as follows:

- Primary Group – Where risk management should focus most of its attention;
- Contingency Group – Where risk management will ensure that contingency plans are in place;
- House Keeping Group – Where basic mechanisms should be in place; and
- Low Group – Where risk is so minimal it does not demand specific attention.

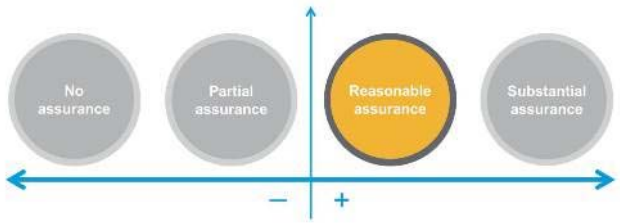
The Force's strategic risks are reviewed by the Force's Risk and Governance Board, which meets every two months. The PCC's strategic risk register is reviewed by the PCC Chief Financial Officer on an on-going basis. Additionally, the Force's and PCC's strategic risk register are presented to the Joint Audit Committee on a bi-annual basis.

Assignment	Actions agreed		
	L	M	H
Subject Access Requests	0	4	1

Objective of the review - To ensure subject access requests have been processed in a timely manner and in accordance with article 15 of the GDPR.

Strategic risk - SR22 – Failure to meet compliance with the UK Data Protection Bill

Overall assurance rating and management actions:



An overall assurance rating of **reasonable assurance** has been given for this review. We have agreed **one high** and **four medium** priority management actions. The high management action related to a lack of operational procedures in place that governed the Force's approach to dealing with SARs.

Context:

Individuals have a right of access to their personal information held by organisations relating to them to help them understand how and why organisations are using their data and that they are doing so lawfully. The powers contained within Article 15 gives individuals the right to request a copy of any of their personal data which are being processed by data controllers. These requests are known as SARs. Following receipt of a SAR an organisation has one calendar month to respond. Failure to comply with these statutory deadlines can lead to fines and sanctions being imposed from the Information Commissioner's Office (ICO).

SARs for the Force are managed by the Information Management Department. The department is led by the Head of Information Management who is also the Force's allocated Data Protection Officer (DPO). The day-to-day receipting and management of SARs is handled by the Information Rights Officer who is supported by an Information Rights Apprentice.

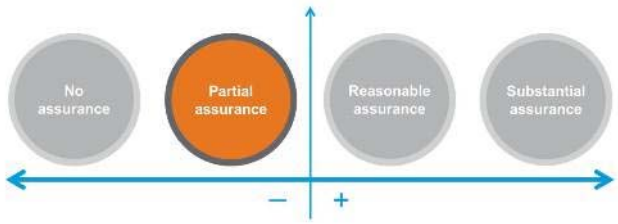
For the 2019 / 2020 financial year, the Force received a total of 354 SARs. Of the 354 requests, 52 (15 per cent) were submitted by either current or ex-staff members of the Force.

Assignment	Actions agreed		
	L	M	H
Overtime	2	6	0

Objective of the review:

To ensure the use of overtime is essential in order to maintain a specific level of service or completion of a specific task and is appropriately reviewed, approved and in line with Police Regulations.

Overall assurance rating and management actions:



An overall assurance rating of **partial assurance** has been given for this review. We have raised **six medium** and **two low** priority management actions. The medium management actions related to:

- The Force did not currently have a comprehensive Overtime Policy in place, which sets out both the relevant Police Regulations, and the internal expectations / controls used within the Force to reinforce an accountable and responsible approach to overtime. Although it was acknowledged that the Force had a policy in draft, we agreed this action to ensure it is completed and includes the actions agreed throughout this report.
- Throughout testing we found instances where the first line supervisors had not received any or adequate guidance, training or clarity on their responsibilities that may contribute to the testing anomalies highlighted in our report.
- A sample of 20 overtime payments found that in two cases the incorrect overtime payment treatment had been applied, resulting in an enhanced rate of pay being received by the claimant, despite not being eligible for this.
- A separate sample was taken for 40 officers who had claimed an enhanced overtime rate and additional benefits, as they had been required to work on rostered rest days or a public holiday. Although testing did not identify any issues with the notification dates as per the Police Regulations, we identified that this may partly be due to the DMS being self-service, permitting officers to submit the 'date they received notification' with no initial controls being in place to mitigate this risk.

Assignment	Actions agreed		
	L	M	H
• The Force has not established values where amounts of TOIL would be considered 'excessive' and be considered for investigation. We tested a sample of 15 part-time officer overtime payments and identified two instances where the officer had not worked in excess of the 40 hours requirement in order to claim an enhanced overtime rate as per the Police Regulations. Context: The Force uses the book on / book off (BOBO) part of the Oracle system for the purposes of recording time worked by police officers. Officers state their time worked via an electronic claim on the time management system including stating any overtime work and the date of when they received the notification to work overtime, where applicable. The Oracle system has built in overtime rules which are operated by the Duty Management System (DMS) and built into the workflows, which facilitate overtime claims being approved by the relevant first line supervisor, who from May 2020 are required to be Inspector or above. In its June 2020 Corporate Financial Monitoring Report, the Chief Finance Officer reported that the wider Force currently has a police overtime budget representing 1.3% of the total Force income budget, with the current monthly forecast for overtime projected to be overspent by £67,000 against an initial annual budget of £1.82m.			

Appendix A – Progress against the internal audit plan 2020/2021

The current Covid-19 situation means that our clients and internal audit are working differently. We understand and recognise the organisations' strategic / primary objectives, and that the developments around Covid-19 will continue to impact on all areas of the organisations' risk profile. We will work closely with management to deliver an internal audit programme which remains flexible and agile to ensure it meets your needs in the current circumstances.

Assignment	Status	Target Joint Audit Committee
Commissioning	**Planning document approved -** Fieldwork scheduled to take place week commencing 14 September 2020	December 2020
Data Quality *	Fieldwork scheduled to take place week commencing 12 October 2020	December 2020
HMICFRS: Recommendation Tracking *	**Planning document issued -** Fieldwork scheduled to take place week commencing 19 October 2020	December 2020
Positive Action *	Fieldwork scheduled to take place week commencing 2 November 2020	December 2020
Follow Up of Previous Internal Audit Recommendations: Visit 1	**Planning document approved -** Fieldwork scheduled to take place week commencing 2 November 2020	December 2020
Human Resources: Wellbeing *	Fieldwork scheduled to take place week commencing 9 November 2020	March 2021
Payroll	Fieldwork scheduled to take place week commencing 16 November 2020	March 2021
Whistleblowing	Fieldwork scheduled to take place week commencing 16 November 2020	March 2021

Assignment	Status	Target Joint Audit Committee
Key Financial Controls	Fieldwork scheduled to take place week commencing 11 January 2021	March 2021
Domestic Abuse *	Fieldwork scheduled to take place week commencing 25 January 2021	March 2021
ICT *	Fieldwork scheduled to take place week commencing 1 February 2021	June 2021
Seized Exhibits *	Fieldwork scheduled to take place week commencing 1 February 2021	June 2021
Purchase and Credit Cards	**Planning document approved -** Fieldwork scheduled to take place week commencing 22 February 2021	June 2021
Follow Up of Previous Internal Audit Recommendations: Visit 2	Fieldwork scheduled to take place week commencing 1 March 2021	June 2021

***** The internal audit plan presented to the Joint Audit Committee on 29 June 2020 was discussed in terms of delivery practicalities in light of the Covid-19 pandemic and if lockdown restrictions continued over the longer term. We have detailed above the reviews where on-site work would be needed to ensure a comprehensive review is completed.

Appendix B – Other matters

Impact of findings to date on 2020/21 Opinions

The JAC should note that the assurances given in our audit assignments are included within our Annual Assurance Report. In particular, the JAC should note that any negative assurance opinions will need to be noted in the annual report and may result in a qualified or negative annual opinion.

To date we have issued four final reports, one of which was a partial assurance (negative) opinion. This will not in isolation result in a qualification to our opinions. We will provide further updates as more reports are finalised throughout the year.

Changes to the audit plan

Detailed below are the proposed change to the audit plan:

Note	Auditable area	Reason for change
1	No changes to date	

Sector Briefings

Since the last JAC meeting, we have issued the following client briefings and we can provide electronic copies to members if required:

- COVID-19 Fraud Risks
- Alert: COVID-19 used as click bait
- Cyber security risk – Remote Working and New Challenges
- Audit and Risk Committees – Navigating COVID-19; and
- The new board agenda - How organisations can better manage their contingency risks.

Appendix C - Key performance indicators (KPIs)

Delivery			Quality		
	Target	Actual		Target	Actual
Draft reports issued within 10 days of debrief meeting	10 days	*10 days (average)*	Conformance with PSIAS and IIA Standards	Yes	*Yes*
			Liaison with external audit to allow, where appropriate and required, the external auditor to place reliance on the work of internal audit	Yes	*As and when required*
Final report issued within 3 days of management response	3 days	*1 day (average)*	Response time for all general enquiries for assistance	2 working days	*2 working days (average)*
			Response for emergencies and potential fraud	1 working day	-

For more information contact

Daniel Harris
Head of Internal Audit

RSM Risk Assurance Services LLP
1 St. James' Gate, Newcastle Upon Tyne, NE1 4AD
M: +44 (0)7792 948767 | **W:** www.rsmuk.com

rsmuk.com