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

Internal Audit Progress Report

15 December 2022

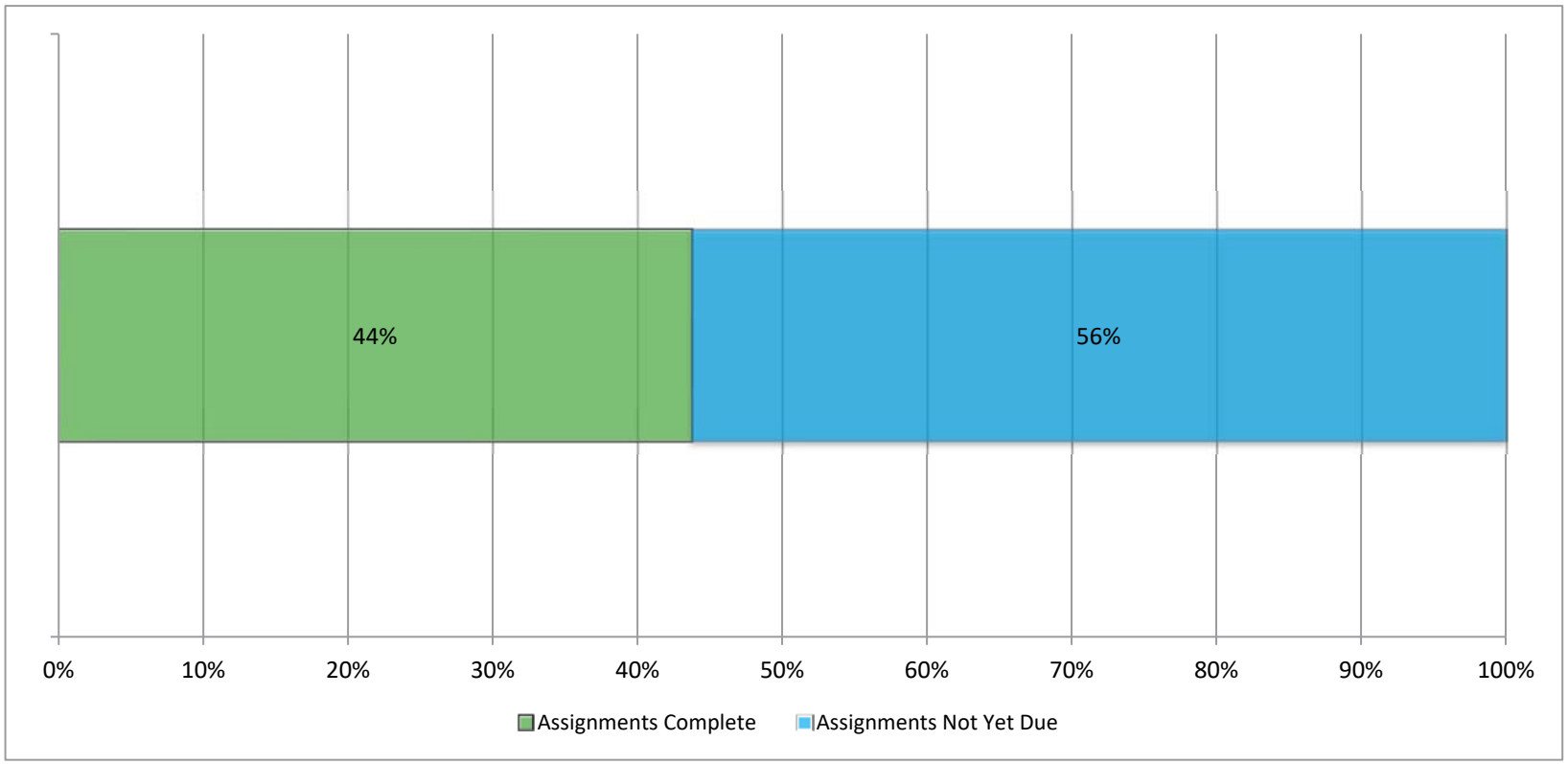
RSM

Contents

1 Introduction

The internal audit plan for 2022/23 was approved by the Joint Audit Committee (JAC) on 30 June 2022.

The graphic below provides a summary update on progress against this plan.



2 Reports

2.1 Summary of final reports being presented to this committee

This section summarises the five reports that have been finalised since the last meeting.

Assignment	Opinion issued	Actions agreed		
		L	M	H
Integrated Offender Management * This review relates to 2021/22	**Reasonable Assurance** 	1	2	0
Follow Up of Previous Internal Audit Management Actions: Visit 1	**Good Progress**	2	1	0
Health and Safety	**Minimal Assurance** 	1	3	5

Assignment	Opinion issued	Actions agreed		
		L	M	H
Key Financial Controls	**Substantial Assurance** 	1	0	0
GDPR	**Advisory Review**	2	2	1

Appendix A: Progress against the internal audit plan 2022/23

Assignment	Status	Target Joint Audit Committee
HR: Training	**Planning document issued** Fieldwork schedule to take place week commencing 5 December 2022	March 2023
Commissioning	**Planning document issued and approved** Fieldwork schedule to take place week commencing 16 January 2023	March 2023
Follow Up of Previous Internal Audit Management Actions: Visit 2	Fieldwork schedule to take place week commencing 16 January 2023	March 2023
HMICFRS: Recommendation Tracking	Fieldwork schedule to take place week commencing 16 January 2023	March 2023
Human Resources: Suspension and Restrictive Duties	Fieldwork schedule to take place week commencing 30 January 2023	March 2023
De-collaboration: CDSOU	Fieldwork schedule to take place week commencing 13 February 2023	June 2023
Vulnerable People	**Planning meeting issued and approved** Fieldwork schedule to take place week commencing 20 February 2023	June 2023
Seized Exhibits	**Planning document issued and approved**	June 2023

Assignment	Status	Target Joint Audit Committee
	Fieldwork schedule to take place week commencing 6 March 2023	
Criminal Disclosure	Fieldwork schedule to take place week commencing 20 March 2023	June 2023

Appendix B: Other matters

Impact of findings to date on 2022/23 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.

We have issued seven final reports to date in 2022/23. Any negative opinions will impact our year end opinions, but may not result in a qualification. To date we have issued two negative opinions (one minimal and one partial assurance opinions) relating to final reports, and both of these will impact our Head of Internal audit opinions, but will not in isolation result in a qualified year end opinions at this stage. We still have another nine reviews to undertake during 2022/23. We will keep the CFOs informed of our remaining audits and any further negative opinions that may impact the year end Head of Internal Audit opinions.

Changes to the audit plan

Detailed below are the changes to the audit plan:

Note	Auditable area	Reason for change
1.	Human Resources: Agency Staff **(Reported to JAC in September)**	Following planning for this review, it was identified the Force have a minimum number of agency staff employed. A such the review has been removed from the audit programme for 2022/23. The Chief Finance Officer (Commissioner) approved the removal of the review.
2	Delivery timescales **(Reported to JAC in September)**	The audit plan which was approved by JAC on 30 June included proposed timings for audit delivery. Management have requested the delivery timescales to be changed for the following reviews: • Human Resources: Suspension and Restrictive Duties. This review was due to commence week commencing 25 July 2022 and has been rescheduled for week commencing 12 January 2023 at the request of management.

		• Seized Exhibits. This review was due to commence week commencing 26 September 2022 and has been rescheduled for week commencing 6 March 2023 at the request of management.
3	Bail Management	On 26 September 2022, RSM met with the CFO – OPCC and the CFO – Chief Constable to discuss the audit priorities for the remainder of the year. It was agreed that Bail Management would be removed from the internal audit programme for 2022/23. Bail management will be discussed as part of the planning for the 2023/24 internal audit programme.
4	Delivery timescales	The audit plan which was approved by JAC on 30 June included proposed timings for audit delivery. Management have requested the delivery timescales to be changed for the following review: • Vulnerable People. This review was due to commence week commencing 14 November 2022 and has been rescheduled for week commencing 20 February 2023 at the request of management.

Appendix C: Key performance indicators (KPIs)

Delivery	Target	Actual	Quality	Target	Actual
Draft reports issued within 10 days of debrief meeting	10 days	*7 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	-

Appendix D: Internal audit assignments reported previously

Reports previously seen by the Joint Audit Committee and included for information purposes only:

Assignment	Opinion issued	Actions agreed		
		L	M	H
Vetting	**Partial Assurance** 	2	2	1
Firearms Licensing	**Reasonable Assurance** 	2	2	0
Cyber Security Review	**Reasonable Assurance** 	0	1	1

For more information contact

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

rsmuk.com

Emergency Services News Briefing

December 2022

Contents

In this edition of our news briefing, we draw attention to some of the key developments and publications in the sector, with particular focus on the latest reports from His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) and the Fire Standards Board new Data Management Standard

Police

Police dismissals to be reviewed

The Home Office will launch a targeted review of police dismissals to raise standards and confidence in policing across England and Wales. The Home Office review will consider:

- the effectiveness of the current system to “dismiss those who fall seriously short of the standards” required by policing and the public;
- the effect of the introduction of changes to misconduct panels, including legally qualified chairs; and
- whether forces are using their powers to discharge officers while they are on probation.

Read more

Over 50,000 female police officers now in forces

The Home Office has highlighted that women now make up over 50,000 police officers in forces in England and Wales. With 15,343 more police hired so far (77% of the target), the government is on course to meet its manifesto commitment to recruit 20,000 additional officers by March 2023. To ensure that forces are able to hire the additional officers needed to keep communities safe, the government has worked with chief constables and the College of Policing to modernise, standardise, and strengthen the recruitment process. All recruits must fulfil the requirements established by the College of Policing.

Read more

Force management statement template and guidance

His Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) has published its latest template for forces to populate alongside updated guidance to support forces. The information required helps HMICFRS inform its inspections of forces’ efficiency, effectiveness and legitimacy, thematic inspections and supplements its monitoring of forces’ performance.

Read more

An inspection of vetting, misconduct, and misogyny in the police service

HMICFRS has published a report following a review of 725 police vetting files and 264 complaint and misconduct investigations. Key findings include:

- there were too many cases where people should not have been allowed to join the police, including officers with criminal records or links to organised crime;
- there were cases where evidence that a prospective officer may present a risk to the public was ignored;
- in some instances, forces consistently failed to implement recommendations contained in inspection reports;
- examples of police officers transferring between forces despite a history of concerning intelligence, complaints or misconduct allegations;
- there were incidents which should have been assessed as gross misconduct that were assessed as misconduct only, or not treated as misconduct at all;
- vetting interviews are used infrequently. Instances had arisen where vetting enquiries revealed concerning information, but forces hadn't interviewed applicants to clarify the issues; and
- HMICFRS found that misogyny, sexism and predatory behaviour towards female police officers and staff and members of the public still exists.

HMICFRS has made 43 recommendations which include:

- updating minimum standards for pre-employment checks;
- establishing better processes for managing risks relating to vetting decisions, corruption investigations and information security;
- improving the quality and consistency of vetting decision-making, and improving the recording of the rationale for some decisions;
- extending the scope of the law on police complaint and misconduct procedures;
- strengthening guidance for forces on vetting processes and relationships and behaviours in the workplace;
- understanding and defining what constitutes misogynistic and predatory behaviour;
- improving how the police collect corruption-related intelligence; and
- improving how the police assess and investigate allegations of misconduct.

Read more

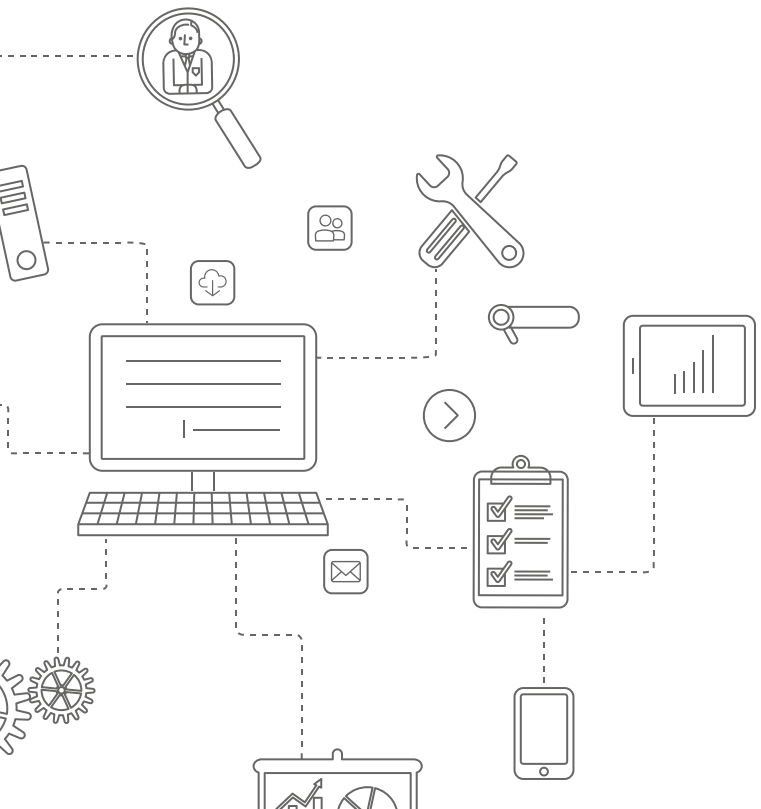
Fire

Economic and Social Value of the UK Fire and Rescue Services Methodology

The National Fire Chiefs Council (NFCC) has launched the Economic and Social Value of Fire and Rescue Services (FRS) Methodology. The methodology has been developed by the Community Risk Programme at NFCC which commissioned Nottingham Trent University to carry out the research. The research was informed by subject matter experts from across the UK FRS and by the Home Office. The methodology includes a report which sets out the value of FRS activities using evidence-based methodologies to calculate the social return on investment and a tool which FRS can input their own data into. A digital version of the tool, using the base methodologies, will be developed for release during 2023.

The methodology will allow fire and rescue services to evaluate and understand the benefit and the financial impact of their response, prevention and protection activities. This will support FRS in their community risk management planning and help to inform their resource allocation.

Read more



Early Intervention Implementation Framework launched

The National Fire Chiefs Council (NFCC) has launched a new Early Intervention Implementation Framework, which is a suite of guidance and tools to assist fire and rescue services in delivering effective early intervention programmes that meet the needs of young people, communities and key stakeholders. The framework includes tools for strategic direction, implementation, monitoring and evaluation and a new strategic Theory of Change which sets out a national core approach for interventions. Within the Theory of Change are seven key steps that NFCC will support FRSs to take. To assist fire and rescue services to use the new framework, a series of virtual sessions are being hosted by the NFCC Implementation Support Team and the Early Intervention workstream.

Read more

Fire Standards Board launches new standard

The Fire Standards Board (FSB) has announced the launch of the 12th professional Fire Standard. Covering data management, it focuses on ensuring that fire and rescue services can deliver excellence to the public by maximising the value of good quality and reliable data. The aim of the Data Management Fire Standard is that services will use data to inform their community risk management planning and other key activities which will contribute to a reduction in risk and improvements in community safety. It is expected that the Standard will deliver an improved quality of service to the public because of their effective use of high quality and robust local, regional and national data to evidence their considerations and decision-making. As with all Fire Standards, there is a corresponding Fire Standards Implementation Tool, designed to support services in assessing how well they already meet the standard and what they may need to consider and act on in terms of their working practices.

Read more

Police and Fire

Being ‘scam savvy’ in the cyber world

Cyber crime is a serious threat to police forces and fire and rescue services. With many of us working online, to protect yourself and your organisation, it is more important than ever that you, as the first line of defence, are aware of scams.

Our Cyber Security 2021 survey found that 20 per cent of organisations had experienced a cyber attack in the last 12 months, and 71 per cent of respondents said the attack was a direct result of the coronavirus pandemic.

95 per cent of cyber security breaches are due to human error, so user behaviour and education is the best way to protect your organisation against many of the most common scams.

To assist providers, we detail some key considerations for securing your IT systems, digital infrastructure, and organisational assets.

Securing your IT environment: Key considerations

Network configuration

- Firewalls are imperative for monitoring, permitting and blocking data. You should have a firewall security policy, detailing the types of rules used and what each rule set does. Firewall rules should be reviewed frequently (in line with policy). The policy should also state how logging and alerts are configured and monitored.

Access controls and passwords

- Strong passwords should be required from all users. Review ‘password history’ controls frequently, to prevent individuals from cycling the same passwords, and consider implementing a lockout threshold of three to five attempts.
- Where possible, implement Multi Factor Authentication (MFA), as without MFA there is an increased risk of compromised accounts.

Security patches and antivirus software

- Antivirus and software updates should routinely be applied and supported by underlying policies and procedures. It’s also important to ensure that all devices have the latest security patches installed and that they are encrypted to ensure confidential data is protected in the event of a cyber-security breach.

Data backup and business continuity

- Backups are essential to ensuring that key data can be recovered in the event of an operational failure or cyber-attack. A backup procedure and policy should already be in place that includes the backup schedule, retention periods, and backup restoration testing schedule.

Has your IT incident response plan been tested recently?

A comprehensive incident response plan is essential, as it will guide a provider’s response to an attack. At a minimum, a formal incident management policy and related processes should be in place, including:

- roles;
- responsibilities;
- accountabilities;
- references to related regulation;
- reporting requirements; and
- explicit examples of what constitutes an incident or
- security breach.

Once documented, a walk-through and other tests of scenarios should be undertaken and extended to relevant third party service providers. The incident management policy should be tested at least every 12 months, and any lessons learnt captured and fed back into the process.

Further information

For more information about how we can help you to protect your organisation, please get in touch with your usual RSM contact.

RSM's Public Procurement Training Level 1

We are pleased to announce that our Public Procurement Training Session will be taking place Friday 3 February 2023. These events have been specifically developed to support practitioners who are starting their procurement careers or for those who need to refresh their knowledge.

Delegates will gain a comprehensive coverage of all key procurement provisions, best practice, and skills to ensure they can confidently manage tender processes. There will be plenty of opportunities to ask questions and also take part in practical exercises, online polls and follow-up surgery.

To book your place on our training session please use the link below:

Register here, Friday 3 February 2023.

Emergency Services Risk Register analysis.

We have begun our latest review of emergency services strategic risk registers. Our latest research aims to identify those key risk areas across police and fire, identifying persistent challenges, together with new and emerging risk areas.

Watch out for our analysis report which will be published in 2023.

Authors

Daniel Harris

National Head of Emergency Services and Local Government

T +44 (0)7792 948 767

daniel.harris@rsmuk.com

Zara Raza

Risk Assurance Technical

zara.raza@rsmuk.com