Police & Crime Commissioner for Lincolnshire & Lincolnshire Police

Internal Audit Progress Report

Presented to JIAC – 22nd February 2023

Prepared by: Mazars LLP

mazars

Contents

01 Summary		3
02	Current progress	4
03	Performance 22/23	5
Performance 22/23		6
A1	2022/23 Plan Overview	7
A2	Reporting Definitions	8
A3	Summary of Reports 2022/23	9
A4	Collaboration Audit Plan 2022/23	13
A5	Statement of Responsibility	14
Contacts		15

Disclaimer

This report ("Report") was prepared by Mazars LLP at the request of the Lincolnshire Police and the Officer of the Police and Crime Commissioner (OPCC) for Lincolnshire and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit the Lincolnshire Police and the Officer of the Police and Crime Commissioner (OPCC) for Lincolnshire and to the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Please refer to the Statement of Responsibility in Appendix A1 of this report for further information about responsibilities, limitations and confidentiality.

mazars

01 Summary

The purpose of this report is to update the Joint Independent Audit Committee (JIAC) as to the progress in respect of the Operational Plan for the year ending 31st March 2023, which was considered and approved by the JIAC at its meeting on 28th April 2022.

The Police and Crime Commissioner and Chief Constable are responsible for ensuring that the organisations have proper internal control and management systems in place. In order to do this, they must obtain assurance on the effectiveness of those systems throughout the year and are required to make a statement on the effectiveness of internal control within their annual report and financial statements.

Internal audit provides the Police and Crime Commissioner and Chief Constable with an independent and objective opinion on governance, risk management and internal control and their effectiveness in achieving the organisations' agreed objectives. Internal audit also has an independent and objective advisory role to help line managers improve governance, risk management and internal control. The work of internal audit, culminating in our annual opinion, forms a part of the OPCC and Forces' overall assurance framework and assists in preparing an informed statement on internal control.

Responsibility for a sound system of internal control rests with the Police and Crime Commissioner and Chief Constable and work performed by internal audit should not be relied upon to identify all weaknesses which exist or all improvements which may be made. Effective implementation of our recommendations makes an important contribution to the maintenance of reliable systems of internal control and governance.

Internal audit should not be relied upon to identify fraud or irregularity, although our procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control will not necessarily be an effective safeguard against collusive fraud.

Our work is delivered is accordance with the Public Sector Internal Audit Standards (PSIAS).

02 Current progress

2022/2023

Since the last update to the Committee in December 2022 we are pleased to report the final report in respect of IT Cyber Security. See Appendix A3 for full details.

We have completed the fieldwork in respect of Stock Control and Core Financials across January and early February and these reports will be issued in draft shortly and the audits of Environmental Sustainability & IT Resilience began in early February.

The remaining audits in Lincolnshire's plans are scheduled to take place across the rest of February and March and the scopes of each review and the dates for fieldwork have been shared.

In regard to the 22/23 Collaboration Audit Plan, the three remaining audits of EMSOT Closedown, Digital Currency and Performance Management have all been issued in draft and are pending management responses. See Appendix 3 for full details.

03 Performance 22/23

The following table details the Internal Audit Service performance for the year to date measured against the key performance indicators that were set out within Audit Charter.

Number	Indicator	Criteria	Performance
1	Annual report provided to the JIAC	As agreed with the Client Officer	N/A
2	Annual Operational and Strategic Plans to the JIAC	As agreed with the Client Officer	Achieved
3	Progress report to the JIAC	7 working days prior to meeting.	Achieved
4	Issue of draft report	Within 10 working days of completion of final exit meeting.	25% (1/4)*
5	Issue of final report	Within 5 working days of agreement of responses.	100% (4/4)
6	Follow-up of priority one recommendations	90% within four months. 100% within six months.	N/A
7	Follow-up of other recommendations	100% within 12 months of date of final report.	N/A
8	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork.	93% (11/13)
9	Customer satisfaction (measured by survey) “Overall evaluation of the delivery, quality and usefulness of the audit” – Very Poor, Poor, Satisfactory, Good, Very Good.	85% average satisfactory or above	100% (3/3) 3 x Very Good

*4-7 days over the ten largely caused by Annual Leave & Auditor Study Leave in Aug & Sept

Performance 22/23

To provide the Committee with further clarity on the status of each audit within the plan below us a suggested further performance information for consideration:

Audit	Date of ToR	Start of Fieldwork	Days' Notice	Exit meeting	Draft Report	Time from Close to Draft Report (10)	Final Management Comments Received	Time to Receive Management Comments	Final Report Issued	Time Taken to issue Final (5)
Archives Man-Follow Up	23-Jun-22	1-Aug-22	28	11-Aug-22	02-Sep-22	17	14-Sep-22	9	14-Sep-22	0
Estates Management	4-Jul-22	1-Aug-22	21	16-Aug-22	02-Sep-22	14	14-Sep-22	9	14-Sep-22	0
Risk Management & Assurance Map	25-Jul-22	22-Aug-22	21	14-Sept-22	03-Oct-22	14	27-Oct-22	19	27-Oct-22	0
IT Cyber Security	12-Sep-22	28-Nov-22	56	20-Jan-23	20-Jan-23	0	1-Feb-23	9	2-Feb-23	1
IT Resilience	12-Sep-22	13-Feb-23	111							
Core Financials	28-Oct-22	3-Jan-23	48							
Stock Control	01-Dec-22	16-Jan-23	33							
Environmental Sustainability	19-Jan-23	6-Feb-23	13							

A1 2022/23 Plan Overview

Audit area	Planned Fieldwork Date	Draft Report Date	Final Report Date	Target JIAC	Comments
Follow Up - Archives Man	Aug 22	Sept 22	Sept 22	Dec 22	Final Report Issued
Estates Management	Aug 22	Sept 22	Sept 22	Dec 22	Final Report Issued
Risk Management & Assurance Mapping	Aug 22	Oct 22	Oct 22	Oct 22	Final Report Issued
Core Financials	Jan 23				Draft Reports to be issued shortly
Stock Control	Jan 23				Draft Reports to be issued shortly
Sustainability	Mar 23				Fieldwork began 6th Feb
Learning & Development	Mar 23				
Data Quality	Feb 23				
Follow Up - Procurement	Feb 23				
Equality, Diversity & Inclusion	Feb 23				
Business Continuity	mar 23				
Follow Up - Wellbeing & Archives Man	Mar 23				
IT Governance & IT Benefits Realisation	n/a				Following Planning meetings these audits have been combined into an IT Resilience Review
IT Resilience	Nov 22	Jan-23	Feb-23	Feb-23	Final Report Issued
IT Cyber Security	Feb 23				Fieldwork began 13th Feb

A2 Reporting Definitions

Definitions of Assurance Levels		
Assurance Level	**Adequacy of system design**	**Effectiveness of operating controls**
Significant Assurance:	There is a sound system of internal control designed to achieve the Organisation's objectives.	The control processes tested are being consistently applied.
Satisfactory Assurance:	While there is a basically sound system of internal control, there are weaknesses which put some of the Organisation's objectives at risk.	There is evidence that the level of non-compliance with some of the control processes may put some of the Organisation's objectives at risk.
Limited Assurance:	Weaknesses in the system of internal controls are such as to put the Organisation's objectives at risk.	The level of non-compliance puts the Organisation's objectives at risk.
No Assurance:	Control processes are generally weak leaving the processes/systems open to significant error or abuse.	Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.

Recommendation Priority	Description
1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose the Organisation to a high degree of unnecessary risk.
2 (Significant)	Recommendations represent significant control weaknesses which expose the Organisation to a moderate degree of unnecessary risk.
3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.

A3 Summary of Reports 2022/23

Below we provide brief outlines of the work carried out, a summary of our key findings raised, and the assurance opinions given in respect of the final reports issued since the last progress report in respect of the 2022/23 plan.

Cyber Security 22/23

Overall Assurance Opinion	Satisfactory

Recommendation Priorities	
Priority 1 (Fundamental)	
Priority 2 (Significant)	2
Priority 3 (Housekeeping)	2

The audit will provide assurance with regards to the Forces ongoing management of Cyber Security. Areas for improvement identified will then be brought to the attention of management and advice will be issued on how particular problems may be resolved and controls reviewed to improve future performance.
The audit objectives are to provide assurance in the following areas:

- Confirmation of the current status of GIRR, Airwave and PSN accreditations.
- Review progress against issues identified during the IT Health check process supporting accreditations.
- Review governance processes for monitoring and discussing cyber security issues including responsibilities, oversight, senior management lead and progress reporting.
- Review cyber security breach policy and incident reporting and investigation processes.
-

The objectives of our audit were to evaluate the adequacy and effectiveness of the Cyber Security Governance systems with a view to providing an opinion on the extent to which risks in this area are managed. In giving this assessment it should be noted that assurance cannot be absolute. The most an Internal Audit Service can provide is reasonable assurance that there are no major weaknesses in the framework of internal control.

We are only able to provide an overall assessment on those aspects of the Cyber Security Governance system that we have tested or reviewed. Testing has been performed on a sample basis, and as a result our work does not provide

We raised two priority 2 (significant) recommendation and the detailed recommendation, finding and management response are provided below:

Recommendation 1 (Priority 2)	1) The Force needs to put greater emphasis and priority on mitigating against the high impact vulnerabilities as stated in the ITHC in a timelier manner. 2) The Force should revise their RAP to be clearer in what end point the action plan corresponds to. 3) The Force should adopt a more proactive vulnerability management approach running Nessus monthly to identify new vulnerabilities to feed into the RAP
Finding	The National Cyber Security Centre (NCSC) recommend that critical/high vulnerability ratings should be resolved within 14 days of release.

	However, there are a number of high impact vulnerabilities which were outlined in the ITHC report (June 2022) which remain outstanding more than five months later. We inspected the remediation action plan (RAP) which the Force uses to monitor the mitigation of the vulnerabilities in the ITHC, but this is not clear in the 'descriptive detail' column as it does not clearly indicate to which devices the vulnerability applies. The Force does not use a vulnerability scanning tool on a regular basis. Whilst Nessus has been acquired, it has not been configured to conduct regular scans to identify potential vulnerabilities that arise in between the annual ITHC. *Risk:* Lack of progress against material vulnerabilities, such as those identified by the ITHC, elevates the risk of a cyber security breach.
Response	1) The Network & Security team continues to be under resourced due to an inability to fill skilled roles within the team. Whilst there are now two dedicated Security Analysts there is a continued impact on risk mitigation as they necessarily must also fulfil Network Analyst functions. Other options are being explored with the support of senior management e.g. contractor support and resource planning efficiencies. This will take time to resolve. Once the resources are in place the Security Analysts will focus exclusively on their primary role ensuring timely resolution of risks. 2) Granularity of reporting within the SharePoint RAP will be improved for the next application specific IT Health Check (ITHC) provisionally scheduled for the end of February. Based on feedback from the next reporting period, changes will then be finalised in time for the next annual ITHC in June. The process of improving the RAP will become part of a continuous feedback loop via Quarterly Security Briefings and the Information Management Board. 3) Monthly vulnerability scans have been implemented as of January 2023. Office 365 logs are also being reviewed. Results will be shared with key stakeholders through reporting activities detailed in 4.4 below. Work is also ongoing with the NMC to look at what other tools can be utilised to share a clearer picture of our current security vulnerabilities. These processes will be formalised in new IT policy and roles and responsibilities made clear via RACI.
Responsibility / Timescale	1) IT Security Analysts - 01/24 2) Force ITSO Initial changes in line with recommendation to include any further local feedback by 31/3/23 3) Security Analysts 01/08/23

Recommendation 2 (Priority 2)	The Force should also revise their emergency plan to include for different types of cyber-attacks and not to generalise their guidance.
Finding	The Force's Cyber Attack Response Plan does not include comprehensive measures or guidance for responding to different types of incidents for example phishing, intruders, or ransomware. *Risk:* Security incidents may not be contained, investigated, and mitigated effectively.
Response	The current plan has previously been reviewed by the National Management Centre and is planned for annual review in February as part of the annual review process. Security Analysts will work with the NMC to review the IT audit feedback and integrate that into an updated plan as appropriate.

Responsibility / Timescale	Security Analysts 01/08/23

We also raised two recommendations of a housekeeping nature:

- The Force should look to track all staff that have read the policies with regular reminders to ensure all policies have been read and understood..

Management noted that this recommendation will need to be discussed in Force to ensure that we balance the risk identified against the resources and money that we have available.

- The Force should evaluate which Key Risk Indicators's and Key Control Indicators's might be relevant and effective. Reports to any control failures should be made to the IMB as well as statistics of how effective current controls are.

Management accepted the recommendation and noted This will be an ongoing process with continuous improvement of the reporting intrinsic to the developing threat landscape. The target date reflects the initial report publication at the next Quarterly Security Briefing with time to implement further feedback enabling us to proceed with a solid peer reviewed reporting framework.

A4 Collaboration Audit Plan 2022/23

Audit area	Forces	Status
EMSOT Closedown	Leics, Lincs, Northants	Draft Issued
EMSLDH Governance	Derby, Leics, Northants, Notts	Final Report Issued
EMSOU - Business Continuity	Five Force	Final Report Issued
EMSOU Risk Management	Five Forces	Final Report Issued
Collaboration Performance Management	Five Forces	Draft Issued
Digital Currency	Five Forces	Draft Issued

A5 Statement of Responsibility

We take responsibility to Lincolnshire Police and the Office of the Police and Crime Commissioner for Lincolnshire for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made. Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or reply for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation amendment and/or modification by any third party is entirely at their own risk.

Registered office: 30 Old Bailey, London, EC4M 7AU, United Kingdom. Registered in England and Wales No 0C308299.

Contacts

David Hoose
Partner, Mazars
david.hoose@mazars.co.uk

Mark Lunn
Internal Audit Manager, Mazars
mark.lunn@mazars.co.uk

Mazars is an internationally integrated partnership, specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories around the world, we draw on the expertise of 40,400 professionals – 24,400 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.co.uk