Office of the Police & Crime Commissioner for Lincolnshire and Lincolnshire Police

Internal Audit Progress Report 2023/24

Audit Committee – 2nd August 2023

Prepared by: Mazars LLP

Date: July 2023

mazars

Contents

1 Introduction

2 Progress to Date

3 Appendices 1 to 4

4 Statement of Responsibility

Status of our Reports

Disclaimer

This report ("Report") was prepared by Mazars LLP at the request of the Lincolnshire Police and the Officer of the Police & 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 & 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 on the final page of this report for further information about responsibilities, limitations and confidentiality.

mazars

01

Section 01:

Introduction

Introduction

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 2024, which was considered and agreed with management on 16 May 2023.

Responsibility for a sound system of internal control rests with the Police & 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).

Background

The purpose of the internal audit plan is to identify the work required to achieve a reasonable level of assurance to be provided by Mazars LLP in compliance with the Public Sector Internal Audit Standards (PSIAS).

The Police & 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 & Crime Commissioner and Chief Constable with an independent and objective opinion on governance, risk management and internal control and their effectiveness in achieving the organisation's 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 Force's overall assurance framework and assists in preparing an informed statement on internal control.

02

Section 02:

Progress to Date

Progress to Date

We have issued the following 2022/23 Final Reports since the last meeting of the Audit Committee:

- Core Financials (**Significant**)
- Stock Control (**Satisfactory**)
- Data Quality (**Satisfactory**)
- Equality, Diversity & Inclusion (**Satisfactory**)
- IT Resilience (**Limited**)

We have issued the following 2022/23 Collaboration Final Reports since the last meeting of the Audit Committee:

- Collaboration: EMSOT Closedown (**Limited**)
- Collaboration: Digital Currency (**Satisfactory**)
- Collaboration: Performance Management **(Satisfactory**)

We have issued the following 2022/23 Draft Reports since the last meeting of the Audit Committee:

- Environmental Sustainability
- Procurement Follow Up

Progress against the 2022/23 Internal Audit Plan is shown in Appendix 1

Progress to Date (Continued)

Due to staffing issues within the Force's Learning and Development department, there is still some fieldwork to complete for the Learning and Development audit for 2022/23 and this has been deferred into the 2023/24 plan.

Progress against the 2022/23 Internal Audit Plan is shown in Appendix 1.

We have begun delivery of the 2023/24 audit plan, with the fieldwork for Firearms Licensing having concluded and draft report to be issued shortly.

Progress against the 2023/24 Internal Audit Plan is shown in Appendix 2.

The dates for several of the other audits in the plan have been agreed including Workforce Planning in September and Core Financials in December. Whilst we are still working to agree the dates for the rest of the audits in the plan, we have provided an indicative month for each audit in the IA plan and will continue to update the committee at each meeting as to the status. The current schedule has been designed for an even spread of audits across the year to prevent a back loaded plan as occurred during 2022/23, with reasons for this previously discussed with the committee.

As in previous years, the collaboration audit plan for 2023/24 has been agreed by the regional CFOs and a copy of the plan is included at Appendix 3. The committee should note the plan is smaller than in previous years to reflect the reduced amount of regional collaboration.

Performance 2022/23

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	In Progress
2	Annual Operational and Strategic Plans to the JIAC	As agreed with the Client Officer	Achieved (Apr 23)
3	Progress report to the JIAC	7 working days prior to the meeting	Achieved
4	Issue of draft report	Within 10 working days of completion of the final exit meeting	27% (3 / 11)
5	Issue of final report	Within 5 working days of agreement of responses	78% (7 / 9)
6	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork.	82% (9 / 11)
7	Customer satisfaction (measured by survey) Very Good / Good / Satisfactory / Poor / Very Poor	85% average satisfactory or above	100% (3 / 3) Very Good

Performance 2023/24

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 (August 23)
3	Progress report to the JIAC	7 working days prior to the meeting	Achieved
4	Issue of draft report	Within 10 working days of completion of the final exit meeting	n/a
5	Issue of final report	Within 5 working days of agreement of responses	n/a
6	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork.	100% (3 / 3)
7	Customer satisfaction (measured by survey) Very Good / Good / Satisfactory / Poor / Very Poor	85% average satisfactory or above	n/a

Definition of Assurance & Priorities 2022/23

Audit Assessment 2022/23

In order to provide management with an assessment of the adequacy and effectiveness of their systems of internal control, the following definitions are used.

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.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Definitions of Recommendations	
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.

Definition of Assurance & Priorities 2023/24

Audit Assessment 2023/24

It should be noted that a slight change to the assurance levels used by Mazars will take place for 2023/24. In order to align with the Government Internal Audit Agency and allow for wider sector comparison the assurance levels used have been updated. The following definitions are used.

Definitions of Assurance Levels		
Assurance Level	**Adequacy of system design**	**Effectiveness of operating controls**
Substantial Assurance:	The framework of governance, risk management and control is adequate.	The control processes tested are being consistently applied.
Moderate Assurance:	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.	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:	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective	The level of non-compliance puts the Organisation's objectives at risk.
Unsatisfactory Assurance:	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.	Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.

Grading of recommendations

In order to assist management in using our reports, we categorise our recommendations according to their level of priority as follows:

Definitions of Recommendations		
Priority	**Description**	**Action Required**
High (Fundamental)	Significant weakness in governance, risk management and control that if unresolved exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium (Significant)	Weakness in governance, risk management and control that if unresolved exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low (Housekeeping)	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.

03

Section 03:

Appendices:

1. Status of Audit Work 2022/23
2. Status of Audit Work 2023/24
3. Status of Collaboration Audit Plan
4. Final Reports Issued

Appendix 1 – Status of Audit Work 2022/23

The table below lists the 2022/23 Internal Audit Plan progress and a status summary for all of the reviews to date.

Audit Area	Fieldwork Date	Draft Report Date	Final Report Date	Target JIAC	Comments
Archives Management Follow Up	Aug 22	Sep 22	Sep 22	Dec 22	Final Report Issued
Estates Management	Aug 22	Sep 22	Sep 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	May 23	Jun 23	Aug 23	Final Report Issued
Stock Control	Jan 23	Mar 23	Jul 23	Aug 23	Final Report Issued
Environmental Sustainability	Feb 23	Mar 23	-	Sep 23	Draft Report Issued
Data Quality	Feb 23	Jun 23	Jul 23	Aug 23	Final Report Issued
Procurement Follow Up	Feb 23	Mar 23	-	Sep 23	Draft Report Issued
Equality, Diversity & Inclusion	Feb 23	May 23	Jun 23	Aug 23	Final Report Issued
Learning & Development	Deferred to 2023/24 Audit Plan				
Business Continuity	Deferred to 2023/24 Audit Plan				
IT Resilience (Originally IT Governance and IT Benefits Realisation)	Nov 22	May 23	Jul 23	Aug 23	Final Report Issued
IT Cyber Security	Jan 23	Jan 23	Feb 23	Feb 23	Final Report Issued

Appendix 2 – Status of Audit Work 2023/24

The table below lists the 2023/24 Internal Audit Plan progress and a status summary for all of the reviews to date.

Audit Area	Fieldwork Date	Draft Report Date	Final Report Date	Target JIAC	Comments
Firearms Licensing	Jul 23			Sep 23	Fieldwork Completed
Learning & Development	Jul 23			Sep 23	
Business Continuity	Aug 23			Nov 23	
Workforce Planning	Sep 23			Nov 23	
Procurement	Sep 23			Nov 23	
OPCC Grants	Oct 23			Feb 24	
Core Financials	Dec 23			Feb 24	
Commissioning	Jan 24			Feb 24	
Health & Safety	Jan 24			Feb 24	
Wellbeing (OHU)	Jan 24			Mar 24	
Governance	Feb 24			Mar 24	
IT Audit (TBC)	TBC			TBC	

Appendix 3 – Status of Collaboration Audit Work

The table below lists the 2022/23 Collaboration Internal Audit Plan progress and a status summary for all of the reviews to date.

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

The table below lists the 2023/24 Collaboration Internal Audit Plan progress and a status summary for all of the reviews to date.

Audit Area	Forces	Status
EMSOU Capital Programme	Five Forces	ToR Agreed
EMSOU Workforce Planning	Five Forces	ToR Agreed
EMSOU HMICFRS Action Plan	Five Forces	ToR Agreed

Appendix 4 – Final Reports Issued

On the following pages, 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 2022/2023 plan and the 2023/2024 plan.

Core Financials 22/23

Overall Assurance Opinion	Significant

Recommendation Priorities	
Priority 1 (Fundamental)	-
Priority 2 (Significant)	1
Priority 3 (Housekeeping)	5

Our audit considered the following risks relating to the area under review:

General Ledger

- Accounting transactions are incorrectly recorded in the accounts.
- Management is not aware of performance issues due to lack of detailed management accounts.
- Missing transactions are not identified due to reconciliations not being completed.

Cash, Bank & Treasury Management

- Missing transactions are not identified due to reconciliations not being completed.
- Receipted monies are not accurately recorded.
- Treasury and other financial decisions are not made based on available cash due to lack of monitoring.
- Investments made do not constitute good value for money.
- Borrowing undertaken does not constitute good value for money.

Payments & Creditors

- New suppliers can be paid without review and verification.
- Supplier details can be amended without review and verification.
- Payments are made without authorisation and not in a timely manner.
- Payments are made for goods and/or services prior to their receipt.
- BACS payments are incorrectly processed.

Income & Debtors

- New debtors can be invoiced without review or verification.
- Invoices are raised incorrectly and/or inappropriately.
- Non-invoiced income is not recorded accurately.
- Credit notes are raised incorrectly and/or inappropriately.
- Income past due is not subject to appropriate debt management actions.
- Recoverable debts are written off inappropriately.

Payroll

- New starters are added to the payroll without review and verification.
- Leavers are not removed from the payroll in a timely manner, leading to overpayments.
- Changes to payroll are not reviewed and verified.
- Statutory deductions are not added accurately to the payroll.
- Voluntary deductions are not added accurately to the payroll in a timely manner.
- Expenses are paid outside of the expenses policy.
- Overtime is paid outside of the overtime policy.
- Payroll payment runs are incorrectly processed.

Other (Cross Cutting Themes)

- Inconsistent approaches are taken to financial activities.
- Systems can be inappropriately accessed.
- Fraudulent activity is not prevented or identified

Core Financials 22/23 (Continued)

We have raised one Priority 2 recommendation which are significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	HR should ensure that both leaver and payroll amendment forms are submitted in a timely manner to Payroll, to minimise the risk of making unrecoverable overpayments and backdating pay.
Finding	Regarding both leavers and amendments to individuals pay, the onus is initially on the line managers to liaise with HR on behalf of their team member, before HR email respective documentation to Payroll to process. Leaver forms and 'Green' (payroll amendment) forms must be submitted before the payroll date of the 16th, in order for Payroll to process in a timely manner. We selected a sample of 10 leavers and 10 payroll variations, to agree to supporting documentation and confirm changes were made correctly and in a timely manner, and noted: • In 2/10 cases where the leaver form was not submitted in a timely manner, including one case where it was submitted after the effective leave date, resulting in overpayments having to be recovered; and, • In 4/10 cases where the payroll amendment form was not submitted in a timely manner, leading to two cases with backdate of pay. Audit did verify for the cases of overpayment that this was recovered within the following months' payslip (due to overtime falling within the next payroll period). Overpayments made amounted to £873.07 and £334.59 respectively.
Risk	Leavers are not removed from the payroll in a timely manner, leading to irrecoverable overpayments. Changes to payroll are not reflected in a timely manner, leading to staff becoming unhappy.
Response	In relation to the leavers identified, one individual in the sample resigned with immediate effect, and another was approved to give less notice than the 28 days due to the circumstances of their leaving and joining another Force. These circumstances mean that due to the payment of salary being two weeks in advance and two weeks in arrears – sometimes the payroll has already been run but changes still occur that affect the relevant pay period and therefore overpayment is unavoidable. In relation to the payroll amendment form, I will monitor this to ensure that where it is within our control, we obtain the information from management in a timely manner, or escalate where this is looking like it will not be the case.
Responsibility / Timescale	Rachel Betts Ongoing

We have also raised five priory 3 recommendations of a housekeeping nature:

- The Force should ensure that all forms are clearly signed by the requestor and authoriser, who are different members of staff, clearly illustrating that segregation of duties is in place confirming the request is legitimate. The Force should ensure all new starter documentation is clearly double-signed and retained, illustrating segregation of duties and appropriate review is in place.

Core Financials 22/23 (Continued)

- The Force should ensure that all monthly reconciliations are reviewed by a second member of staff and clearly noted within the reconciliation.
- The Force should remind staff of the need to double sign supporting evidence (e.g. Income Batch Header sheet) to clearly evidence receipted monies are subject to a verification check.
- The Force should save evidence of authorisation of investments to a shared area, to avoid the risk of inaccessibility following a staff member leaving.
- The Force should update their 'Creditor Invoice Processing Policy' to include specific examples of where instances would fall under categories not requiring a purchase order; this would ensure a consistent approach is taken. A review of the 'Credit Control Policy' should occur promptly and the Force should ensure review of all policies occur regularly and/or when stated within the policy.

Management agreed with the recommendations and timetable for implementation was June 2023

Stock Control 22/23

Overall Assurance Opinion	Satisfactory

Recommendation Priorities	
Priority 1 (Fundamental)	-
Priority 2 (Significant)	2
Priority 3 (Housekeeping)	4

Our audit considered the following risks relating to the area under review:

- The Force has clear policies and procedures for the management of stock.
- Roles & responsibilities for the management of stock is clearly assigned and understood.
- There are appropriate security controls in place at the locations where stock is held and stock rooms are appropriately equipped to prevent any damages.
- The Force have a robust stock take programme to ensure accurate records of the stock held are kept.
- The Force utilise stock reports to ensure replacement of stock is ordered in a timely manner and any potential wastage is minimised.
- The purchase of replacement and additional stock is correctly authorised.
- The Force have a robust process in place for the write off of stock.
- Appropriate mechanisms are in place for the return of and subsequent disposal of any police branded items.
- Management information is produced to allow show effective stock control is taking place.

We have raised two Priority 2 recommendation which are significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	The Force should produce clear and accurate guidance on the completion of stock takes. This should include information around record keeping, the level of discrepancy on the system and any amendments to systems following identification of discrepancies. The Force should remind Stores staff of the importance of updating the system to reflect any changes made upon fitting.
Finding	Audit were informed that the Force intends to complete stock takes of the Stores on an annual basis at financial year end. Stock takes are completed by volunteers, from other departments, excluding stores staff, with the most recent being completed in March 2022. Prior to this stock takes had been paused for three years as a result of the COVID-19 pandemic. Review of the stock take reports from the March 2022 process highlighted weaknesses relating to the audit trail retained. In all instances there was no record of the individuals responsible for completion of the count nor was secondary sign off recorded to validate their accuracy. Furthermore, the lack of up to date documented procedures for the completion of stock takes, including investigation/adjustments for discrepancies, does not facilitate consistency of approach. We selected a sample of 11 stock item types with a total of 248 items and reconciled actual stock levels to reported levels within t-Police, noting a total discrepancy of 3.23% at a value of £265.29. It was noted through discussion with stores staff that discrepancies can occur when officers requested uniform/equipment of a specific size and then changed this upon fitting at the stores. Where this change

Stock Control 22/23 (Continued)

Finding	is not recorded and updated on t-Police, this results in overstating of one item's quantity and understating of another.
Risk	Force is not aware of the level of uniform and other stock it holds.
Response	Some guidance is in place but accepted it is out of date and is required to be updated. Stock records from the 2023 audit do include records signed by those who undertook the stock take and this process will be incorporated into the updated guidance.
Responsibility / Timescale	Business Support Manager End Q2 2023/24

Recommendation 2 (Priority 2)	The Force should investigate the discrepancy of the write off figures to ensure the correct figure has been processed. The Force should have agreed guidance for the write off of stock. The Force should ensure sufficient audit trail is retained for any review, approval and amendments of stock write offs.
Finding	From discussion with management, we were informed that there is currently no defined procedure for the write-off of stock available to HQ Stores staff. This is in contradiction to the most up to date Financial, Contract and Procurement Regulations for the Force which inform that the Force CFO, in conjunction with the Strategic Partner, shall prepare guidance relating to the manner in which stocks and stores are to be administered. Additionally, it is of note here that reference to the Strategic Partner demonstrates the obsolescence of the Financial, Contract and

Finding	Procurement Regulations available as the Force no longer utilises G4S. We assessed the most recent stock-write off for completion in line with Financial Regulation 27 and observed the following issues: • We were unable to verify confirmation of write off figure by the Chief Constable due to a lack of evidence available. • The value of the write off was not consistent across the evidence provided. Email evidence captures the value of the write off previewed by the Head of Finance as £5,711.51, however the email requesting approval from the CFO on the same day captures the write off value as £6,918.21. Upon request, the Force were unable to provide supporting evidence to explain the increased value of the write off.
Risk	There is inconsistent approach in relation to stock write offs resulting in misreporting of actual figures in financial statements and mandatory returns.
Response	In accordance with the Finance & Contract Regs (FR27 – Write-off of Stocks & Stores), during the Strategic Partnership, a report was always submitted to the CPT for approval to write off any stock. This was reviewed by the CPT Contract Manger and submitted for approval to the OPCC's CFO / Force CFO depending on value of write-off being sought. As the CPT has now disbanded, a revised guidance note will be documented – this has previously been provided by the Deputy Finance Officer / Head of Finance.
Responsibility / Timescale	Head of Finance End Q2 2023/24

Stock Control 22/23 (Continued)

We have also raised four priory 3 recommendations of a housekeeping nature:

- The Force should continue to develop and update the Stores procedures notes and guidance to Stores staff.
- Stores Assistant job description to ensure it accurately reflects staff responsibilities so that these are clear when replacing staff on a temporary or permanent basis.
- The Force should ensure that there is guidance produced and available to officers for returns of items to HQ Stores. The Force should investigate the ability to perform reconciliations of returned items against issued stock records to ensure all police branded uniform/equipment is accounted for.
- The Force should consider producing regular MI related to stores performance. MI should be submitted to an appropriate forum to be discussed and actioned as necessary. Performance Indicators could include but not be limited to:-
  - Spoiled Stock
  - Availability of stock
  - Order cycle time

Management agreed with the recommendations and timetable for implementation was End Q2 2023/24

Data Quality 22/23

Overall Assurance Opinion	Satisfactory

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

Our audit considered the following risks relating to the area under review:

- There is an appropriate governance structure in place to evaluate data quality at the Force, including that over individual systems, the Force as a whole and participation in regional systems.
- The roles and responsibilities for ensuring data quality within the Force are clearly stated, communicated and understood.
- There are clearly defined terms of reference within the data quality governance structure.
- For a sample of key systems, there is appropriate guidance/training in place on how to record data correctly and accurately within the system and this is appropriately communicated to all system users.
- The guidance and training is regularly reviewed and updated to ensure that best practice for maintaining data quality is up to date.
- The Force put in place appropriate controls within systems to ensure data quality can be maintained.
- Appropriate consideration to data quality is given for key projects that the Force is engaged with, including the G4S Staff/Data Transfer and NICHE Cloud projects.
- This includes appropriately designing systems with controls to minimise poor data, such as mandatory fields and data validations.
- The right staff and skill sets are utilised within the projects to ensure that data quality concerns are addressed.
- The data quality considerations are correctly timetabled into the project to ensure issues are addressed in a timely manner.
- The Force gain assurance that data quality issues within IT projects are being appropriately addressed.
- The Force have appropriate reporting mechanisms that demonstrate levels of data quality across its systems.
- There are regular reporting mechanisms to ensure the Force have appropriate oversight of data quality across its systems.
- There are robust processes in place for the Force to review their data against national benchmarking data and / or other areas of best practice.
- Lessons learnt and best practice approaches to the correct and accurate recording of data are shared and communicated with system users.

We have raised one Priority 2 recommendation which is significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	The Force and OPCC should implement data quality training modules as part of key systems training (i.e., NICHE, T-Police, etc.) that covers general data quality issues, common errors within these systems and the impacts of data entry and/or record linkage errors.
Finding	Data quality is integral to the integrity and validity of information used by the Force and OPCC in both policing and non-policing operations. Therefore, it is important that all users who can create information are appropriately trained and have appropriate guidance to carry out this function. It has been noted that the training provided to users of specific systems (i.e., T-Police and NICHE) includes limited inclusion for data quality and does not include any discussion regarding broader data quality issues or any of the impacts of inputting erroneous data. There is also no general training on data quality provided to staff and/or officers to support the limited data quality training provided

Data Quality 22/23 (Continued)

Finding	within specific system training. And, as has been noted below, there only seems to be guidance documentation in place regarding data quality for NICHE and not other systems, such as T-Police. Additionally, within some systems it is possible to link records and previous audits across different Forces and systems have noted that this can lead to data quality issues if not appropriately trained.
Risk	Incorrect data entry or linkage can lead to errors in operations and damage to reputation and/or finances.
Response	This is work being undertaken by Methods. They are devising workshops, which can be used as a training package, as part of the linked data strategy which covers data literacy and includes data quality and it's importance. This incorporates Information Asset Owner (IAO) Training, detailing how these roles and Heads of Service are custodians of the data within the systems they 'own'.
Responsibility / Timescale	Head of IMU December 2023

Recommendation 2 (Priority 2)	The Force should ensure that information from the Regional Data Quality team is reported to the Information Management Board and any issues are escalated as required to the Chief Officer Team. Additionally, any issues, recommendations and/or learning presented should be reviewed by the Information Management Unit to determine how these can be rectified or implemented by the Force and/or OPCC.
Finding	Benchmarking is an important tool for identifying areas of best practice and areas for improvement. Currently the Force engages with the Regional Data Quality team regarding data quality issues within the regional NICHE system and from the national PND Data Quality Dashboard. However, this information is not reported back into the Information Management Board to be utilised in the identification of areas of focus and does not inform data quality strategies within the Force.
Risk	The Force is unaware how it's performing in data quality and cannot identify areas of best practice, areas for improvement or lessons learned.
Response	This is already a standing item at IMB. The most recent IMB in May, this was discussed and reported on. It is shown as PND dashboard, but DQ is part of that update and reported to the DCC and CDIO and escalated as needed by DCC and CDIO to Chief Officer Team. The Information Management Unit already review the PND Dashboard document that details DQ issues and will implement and rectified as required.
Responsibility / Timescale	Completed

We have also raised one priory 3 recommendations of a housekeeping nature:

- The Force and OPCC should create further guidance documents for each system in use to provide quick hints, tips and "cheat sheets" for ensuring data quality and integrity is maintained across all systems. This could include how to report data quality issues, how to record transactions in T-Police, how to record found/seized property in NICHE, etc.

Management agreed with the recommendations and had completed actions against this by the publication of our final report.

Equity, Diversity & Inclusion 22/23

Overall Assurance Opinion	Satisfactory

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

Our audit considered the following risks relating to the area under review:

- There are inadequate equality, diversity and inclusion (EDI) strategic and operational quality assurance structures and processes.
  - The Force has an approved policy strategy in place to ensure social diversity, inclusion and equal opportunities for staff and related parties in accordance with good practice guidance.
  - The Force can demonstrate that the overarching Policy is replicated / adopted and operationalised across the Force.
  - The strategy covers its legal and statutory responsibilities, that help support EDI; and allows the Senior Leadership team to be aware of its statutory responsibilities.
- The governance structure in place is not appropriate in supporting the strategy and does not provide sufficient challenge.
  - The governance / organisational structure is appropriate and shows a clear and visible commitment to promoting EDI, e.g. having a dedicated EDI working group and designated individual responsible of EDI.
- The Force does not identify, monitor and complete actions in relation to EDI targets.
  - Targets and actions in relation to EDI have been clearly defined and are appropriate for achieving the strategy aims.
  - The Force maintains an EDI Action Plan and can demonstrate that actions with this are being reviewed, worked towards and completed transparently.
  - The Action Plan sufficiently covers identified gaps across all key ED&I stakeholders, including People, Data, Processes, and Impacts.
  - The Force reviews performance in relation to EDI on a sufficiently regular basis to ensure that cultural changes can be tracked and change is identified and reported.
  - The Senior Leadership and other relevant governance forums (e.g. steering groups and EDI programme Boards) team have oversight of the completion of actions.
- Data collection and monitoring processes are limited so that the Force does not have effective oversight of its potential barriers to equality.
  - The Force has appropriate methods of regular data collection, analysis and reporting.
  - The Force holds a comprehensive up to date recorded of staff data including disclosure rates.
  - The Force has set targets for staff data disclosure rates and where these are not achieved, plans to increase disclosure have been set out.
  - The Organisation uses categories recommended by the Equality & Human Rights Commission (or similar) to monitor the breakdown of staff.
- Staff are unclear of the Force's approach to equality, diversity and inclusion.
  - Training has been provided to staff members in relation to EDI on a sufficiently frequent basis to achieve the objectives of the Policy / Strategy.
  - The content of training provided is accessible, relevant and up to date.
  - EDI guidance, resources and working groups are well known and easily accessible to staff.
- The Senior Leadership Team does not have sufficient oversight of EDI related aims and progress.
  - There is a clearly defined reporting framework, where all varying levels of the business receive regular reporting in relation to EDI.
  - The content of what is reported is appropriate, comprehensive and allows senior leadership to understand the current processes in place and so can provide sufficient challenge and direction.

Equity, Diversity & Inclusion 22/23 (Continued)

We have raised two Priority 2 recommendation which are significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	The Force should implement an EDI Policy, providing a single point of reference for individuals to learn about the Force and its relationship with EDI.
Finding	The Force do not have an overarching EDI Policy in place. Whilst we confirmed the Force have an approved EDI Strategy in place, with clear links to the Force-wide 'Making Lincolnshire Safe' Strategy and the Police and Crime Commissioners Police and Crime Plan 2021-2025, the Force do not have an approved policy which outlines how the Force supports EDI and ensures it is embedded within the organisation. It is good practice for an organisation to have a set EDI policy, as it provides a single place for individuals to learn about both the Force's objectives on EDI and the practices it has implemented to support it in doing so.
Risk	Staff are unaware of the Force's approach to equality, diversity and inclusion.
Response	EDI Team can develop an EDI Policy which will be an overarching document that captures the recommended contents.
Responsibility / Timescale	Head of EDI Q4 2023

Recommendation 2 (Priority 2)	The Force should deliver continuous and regular EDI training to their staff (this can be either formal or informal), ensuring content is relevant, focused and engaging. The Force should ensure logs of training completed are held for both officers and staff, allowing them to verify whether training is successfully completed as per their induction.
Finding	Induction training delivered at the Force includes some exposure to EDI related content. However, there exists no continuous forms of formal training with respect to EDI. Induction training at the Force effectively takes two forms: one tailored towards police officers and the other tailored towards police staff. Student officers must undertake a formal twenty-week induction period within a classroom, which includes coverage of some EDI modules. Training for police staff is primarily accessed through College Learn, an online training platform administered by the College of Police, which also includes mandatory EDI modules. We established through conversations with the Head of EDI and Director of People Services that there are no forms of regular, continuous training with respect to EDI. Staff are able to revisit the modules previously completed, however there is no mandatory obligation to do so. Audit noted through review of the 'EDI Delivery Planner', that the Force have plans to increase informal training delivered to staff, through increased guest speakers / webinars, to ensure staff have continuous access to EDI resources. Audit were unable to sample test completion rates of EDI training. The Force do not hold training logs for student officer induction completions, meaning a sample could not be selected. With respect to online training, the Force were unable to extract completion rates

Equity, Diversity & Inclusion 22/23 (Continued)

Finding	from College Learn due to the Force Administrator (responsible for the management of College Learn) recently leaving the organization.
Risk	Staff do not receive continuous forms of training and are therefore unaware of current EDI matters. The Force are unable to verify whether EDI training is completed by their staff.
Response	We are working with Erin Bell to develop our approach to specific EDI Training and EDI issues within other training courses to ensure content is relevant. In the short term (<12months) the force is developing our capability to utilise T-Police and then ultimately developing a new Learning Management System – LMS (12-24 months). Logs of completed training are held, but it is not currently a straightforward process to maintain oversight of EDI inputs, completion rates and time taken, which should be resolved with the better utilisation of T-Police and then replacement LMS.
Responsibility / Timescale	Head of Learning & Development May 2025

We have also raised two priory 3 recommendations of a housekeeping nature:

- The Force should ensure all elements are correctly populated for activities listed within the 'EDI Delivery Planner'.
- The Force should implement measures to address nil rate responses, most notably for Police Staff, by emphasising to their workforce the significance of the data for decision making and creating a more inclusive environment.

Management agreed with the recommendations and timetable for implementation was Q4 2023.

IT Resilience 22/23

Overall Assurance Opinion	Limited

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

Our audit considered the following risks relating to the area under review:

- IT Resilience – People, process and technology perspective including high level review of the IT architecture and technology in place including remote working.
  - Failover and replication arrangements
  - Single points of failure
  - Monitoring / alerting to detect failure
  - Preventative maintenance – Monitoring of asset support status, strategy for asset refresh
- Linkage/alignment to Disaster Recovery and Business Continuity processes.
- Management reporting related to IT resilience including availability, major incidents and reporting resilience risk and the mitigating actions taken by the Force.

We have raised one Priority 1 recommendation which is fundamental, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 1)	The Force should implement a formal testing procedure annually for all critical IT equipment, Uninterruptible Power Supply, air conditioning systems and generators.
Finding	There are no formal testing procedures for the environmental services that support the data centre and other server rooms at Lincolnshire HQ. Although most components are serviced twice a year, there is a lack of testing to ensure all components are resilient in the event of a serious incident. We acknowledge that the Force is looking to test the generator on load which will take place as part of the next scheduled service. However, at the time of visit no testing had taken place.
Risk	Whilst the on-site data centre fulfils a secondary role, the server room that supports the Force control room is critical. For example, if this room suffered a loss of power or equipment overheated leading to loss of service, the operation of the Force control room could be affected.
Response	We have had a full test of this whereby our site was run on generators for 3 days – this was as part of planned power maintenance not for testing purposes. Estates do test the generator (I believe Quarterly) for the whole site resilient power, so we are currently already testing this. This is not a formal IT procedure however, but it is in essence testing exactly what is required – this may just need to be formalised for IT testing as part of this.
Responsibility / Timescale	IT / Estates Ongoing

IT Resilience 22/23 (Continued)

We have also raised two Priority 2 recommendation which are significant, the full details of the recommendation and management response are detailed below:

Recommendation 2 (Priority 2)	As planned, the Force should review all IT architecture to determine SPOFs. The Force should follow through with its plan to install a dual active/passive SD WAN capability between Force HQ and Azure. The Force should identify subject matter experts and whether these are key person dependencies and where this is noted look to cross pollinate information across other team members. Where this is not feasible, alternative strategies should be employed, such as using a call-off support contract with a third party. As planned, the Force should update their telephony communication system.
Finding	The Force is yet to perform a review of their own Single Points of Failure (SPOF), but plans are in place to complete this as part of a broader review of IT Architecture. However, from our enquiries we note that there are three known single points of failure within the Force: • The connection to Azure that hosts Niche and Pronto is a single link from Thurrock. Whilst a VPN from Lincolnshire HQ could be used as a redundant connection, there is no automatic failover, that would activate this if the Thurrock link failed. Management informed us that planned improvements to the network over the next few months will shortly see this issue resolved. • We were informed that there are many subject matter experts who are also key person dependencies such that if they were to leave the Force, remaining staff members could have difficulties in supporting systems. • The PABX analogue telephony system is outdated, though with the introduction of other forms of voice calling the risk of failure may be limited. We note that the Force plan to replace this shortly with a new digital telephony system that has adequate resilience to cover critical services such as 999/101 etc.
Risk	IT services cease to operate when faults to underlying IT equipment, networks or critical applications occur and stand-by services are not in-place to provide a service. If such faults affected the network, the force would be unable to receive and manage new incidents reported by the public.
Response	We have started the implementation of SD WAN which is the solution that will take over for the Azure VPN and this will make it a resilient service. Telephony is also undergoing a full review and all old analogue kit will be swapped as part of the wider national analogue decom. Analysis on SPOF and relevant documentation for knowledge sharing is an ongoing task – due to staffing constraints we have this will take some time to do a full audit / risk assessment and designs for resilience implementation where required. Putting down 6-month target for this due to the size of work required and current restraints on staffing.
Responsibility / Timescale	IT December 2023

IT Resilience 22/23 (Continued)

Recommendation 2 (Priority 2)	The Force should review the applications catalogue, including; • The criticality tiers for each IT system should be aligned with the recovery time objective and targets found in the business continuity plan and service level agreement. • The adequacy of resilience measures to determine the residual resilience risk, and from this determine if further mitigation strategies need to be developed/implemented.
Finding	The application catalogue provides an overview of all applications and the importance of each as denoted by a system of tiers. We were informed that management plan to review the importance of each system as the previous tiering system is out of date and was inherited from G4S. Although, the application catalogue includes a resilience assessment of each application, management informed us that this requires further review and we also noted that there is no assessment of residual risks that are not mitigated by the measures already in place.
Risk	IT resilience requirements do not align to the needs of the wider business. Nonalignment to the wider business can cause discrepancies in IT resilience goals.
Response	A wider engagement with all business areas that have association with various applications in use across the force will be undertaken to determine the support and resilience requirements, be that for 'standard' business hours and out of hours critical support. This will form the basis of the appropriate replacement tier mechanism and determine the appropriate response for mitigation.
Responsibility / Timescale	IT Service Delivery December 2023

Collaboration – EMSOT Closedown 2022/23

Overall Assurance Opinion	Limited

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

Our audit considered the following risks relating to the area under review:

- The project has an appropriate governance structure in place
- A project plan has been approved by all Forces within the collaboration unit.
- The financial impacts for each Force within the collaboration unit, have been accurately calculated & communicated and agreed by the Forces.
- The progress status of the project is reporting in line with the agreed timescales
- Any variance from timelines have been reported on and actions put in place to ensure the project remains on schedule.
- The staged sign off of the project has been authorised correctly.
- The progress of the project is being accurately reported on and has supporting documentation in regard to current status.

We have raised two Priority 1 recommendations, which are fundamental, and three Priority 2 recommendations, which are significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 1)	For future projects regular reporting of progress should be conducted at the appropriate governance level, which includes measuring of progress against a clear predetermined plan. Measurable metrics should be produced to allow for effective monitoring of progress.
Finding	Within the ToR there is an estimated timescale for the dissolution of EMSOT, commencing in Q1 2022 with a forecasted end of March 2023. Audit were also provided with a Project Plan which provides 16 individual items, with their own duration, start date and finish date. However, from review of the Project Plan it was unclear what certain items related to, for example Scoping Meeting was listed with a duration of “1 day?” and a start and end date of 22/02/2022. The item included no further detail. Given this, audit were unable to reconcile the Project Plan to the Project Log, and could therefore not assess whether progress recorded in the Project Log was consistent with the timings listed in the Project Plan. Minutes are a useful tool to document decisions made by committees and boards, as well as ensuring accountability for any decisions. Audit were informed by management that no minutes were maintained for any of the meetings held by the EMSOT Closedown Project Board. Whilst there is a Project Log maintained which includes the risks, issues, actions and decisions related to the project, the decisions tab only includes seven items, and some are not provided with a rationale. As such, it has not been possible to ensure that all the duties of the board have been performed appropriately. Furthermore, the ToR states “Governance will move from the SMB to a regional project board and the progress will then be reported back to SMB”, however no evidence of reporting from the Project Board to the Strategic Management Board was provided.

Collaboration – EMSOT Closedown 2022/23 (Continued)

Finding	Finally, audit noted that ToR states the function of the Project Manager as to "Ensure that the project delivers within time, budget and agreed quality standards". Audit inquired as to the nature of the quality standards and were informed by the Project Manager that these related to how the staff were treated during the process. However, no metrics were mentioned with regards to how this was monitored, and audit were provided with no evidence to support consideration of how staff were treated and any resulting redundancies.
Risk	Ineffective reporting reduces the oversight of governance groups, as well as the ability for the relevant Forces to be held to account.
Response	The ACC lead reported to the SMB when this sat, but SMB meetings themselves were cancelled so the reporting was more person-to-person; ACC to SMB members outside of a formal meeting. The work of dissolution was conducted more on a 'task and finish' basis where changes were made at an operational level as expediently as possible in each area. The project plan therefore only provided a framework within which these tasks were completed, the operational leads in each area completing the necessary work within as short a timescale as possible. It was all completed well ahead of 'schedule' leaving only the IT Chronicle work stream outstanding. However, we appreciate that this meant this progress reporting was not fully reflected in the documentation.
Responsibility / Timescale	Ongoing ACC

Recommendation 2 (Priority 1)	For future projects financial arrangements should be clearly agreed and documented at the commencement of any closedowns. Budget forecasts should be clearly documented and scrutinised by the relevant governance committee.
Finding	The Section 22 in place for EMSOT includes the following apportionment ratio: • Lincolnshire 44.9% • Lincolnshire 25.9% • Lincolnshire 29.2% Audit were informed by management that those apportionment ratios were still those used during EMSOT Closedown. This was supported by a monthly EMSOT finance summary report, which includes the salary costs and Force specific expenses, apportioned to the above ratio. However, no evidence was provided with regards to the EMSOT budget for 2022/23, nor any specific agreement related to financial arrangements for the Closedown project.
Risk	Financial arrangements are unclear. Assets may be misappropriated.
Response	Agreed
Responsibility / Timescale	Ongoing ACO (Finance & Resources)

Collaboration – EMSOT Closedown 2022/23 (Continued)

Recommendation 3 (Priority 2)	For future projects minutes should be maintained for all meetings conducted by any committee or board of a collaboration unit. Where the frequency of governance meetings is changed from that listed in the related ToR, a clear record of the decision should be maintained, and that should be reflected in the ToR.
Finding	Audit were provided with an Terms of Reference (ToR) related to the EMSOT Closedown project which stated that the basis of the document was based on instruction from the Chief Constables of each of the respective Forces. The ToR notes the existence of a SOT Disaggregation Project Board (Project Board). The Project Board is accountable for ensuring the following: • That the project remains on track; • Status and progress are reviewed against the project plan on a regular basis; • Key risks and issues are discussed and managed; • Financial aspects are reviewed and discussed; • Benefits are defined and realised; • Business change is effectively implemented; and, • Effective links with force implementation teams are maintained. As previously noted in Recommendation 1, no minutes were maintained for the Project Board, and as such audit were unable to assess whether the Board performed their duty with regards to reviewing against the Project Plan on a regular basis, as stated in the ToR. Additionally, within the ToR produced for the EMSOT Closedown project, it is explained that meetings should be held monthly, but that this will be reviewed to ensure that the frequency is appropriate.

Finding	From review of the instances of the meeting evidenced by meeting invites, of which we note only five meetings took place between 06/12/2021 to 06/06/2022, there was a gap of three months between 07/03/2022 and 06/06/2022. Audit were informed that the meeting in June was the final such meeting conducted by the Project Board, at which point it was dissolved. However, within the “Decisions” tab of the Project Log, audit note that the final decision was dated 19/12/2022.
Risk	There is no accurate record of decisions made by the Project Board, and limited capacity for the Board to be held to account.
Response	Recommendation noted with regards the keeping of minutes. It should be borne in mind that minutes are usually kept, however with respect to this project, it was the explicit decision of the SRO that this be kept light touch project management style and that we only keep actions and decisions. Noted re frequency of meetings.
Responsibility / Timescale	Ongoing ACC

Collaboration – EMSOT Closedown 2022/23 (Continued)

Recommendation 4 (Priority 2)	For future projects any change of senior leader for the project should be formally agreed, documented and handover evidenced.
Finding	The ToR includes a Superintendent under the role of Overall SOT Ops Lead, for which the function is listed noted as “Business lead for the disaggregation of SOT”. However, audit were informed that the individual previously listed as Overall SOT Ops Lead retired and was not replaced since it was felt there was not enough work to justify a replacement. Audit was provided with limited evidence to support an appropriate transfer of the responsibilities of the Business Lead to an alternative individual nor were audit informed of the date of retirement.
Risk	There is a lack of clarity regarding the leadership of the project, leading to a lack of ownership of risks and actions, and an ineffective dissolution of collaborations.
Response	Fully understood. In relation to this project, there was not handover as there was no new officer to hand over to. The Supt lead retired but the function that person fulfilled had essentially ceased so the project role became redundant. This could have been documented in the project log though.
Responsibility / Timescale	Ongoing ACC

Recommendation 5 (Priority 2)	For future projects it should be ensured that the project log is regularly and frequently updated to ensure it is an accurate reflection of project status.
Finding	At the time of audit we were provided with a Project Log for EMSOT Closedown, which lists the risks, actions, issues and decisions relating to the project. From our review of this log, audit noted that risk 8 regarding the departure of the Lincolnshire ACC lead is listed as open, although audit was informed by the Project Manager that this individual had in fact been replaced, and that the risk was therefore closed. However, no such actions were included with the risk. Additionally, an ongoing issue and action regarding the transfer of personnel training data from Chronicle, the system used to log training data for EMSOT, to individual systems for the three respective forces was present. Audit were informed at the time by the Project Manager that Lincolnshire and Lincolnshire do not currently have a system to export the data to, and as such the issue is still outstanding. Subsequently after draft report issue an update project log was provided that addressed the outstanding issues.
Risk	Inaccurate and outdated audit trails are maintained, leading to a lack of oversight and accountability regarding actions, issues and risks. Responsibilities regarding the monitoring and ownership of actions are not kept up to date, leading to a lack of ineffective completion of actions and mitigating of risks
Response	As noted above, a more accurate project log could have been kept and this will feed into learning for future projects.
Responsibility / Timescale	Ongoing ACC

Collaboration – Digital Currency 2022/23

Overall Assurance Opinion	Satisfactory

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

Our audit considered the following risks relating to the area under review:

- The roles & responsibilities for the handling of digital currency at the Force/Unit are clearly stated.
- There are clear policies, procedures and guidance available at the Force/Unit for the handling of digital currency.
- The Forces/Unit have appropriate recording mechanisms to identify all digital currency that is held.
- Where digital currency is held by the Force/Unit it is done so in line with best practice & guidance.
- The associated risks to the Force/Unit to investigating, handling and storing digital currency are identifies, recorded and appropriately managed.

We have raised one Priority 2 recommendation, which is significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	Derbyshire, Lincolnshire, Lincolnshire, Lincolnshire and EMSOU should ensure that policy, procedure and guidance documentation is in place and updated in line with NPCC guidance and Komainu storage and realisation processes.
Finding	For Derbyshire, Lincolnshire, Lincolnshire, Lincolnshire and EMSOU - we have noted that policies, procedures and guidance documents are being updated following the issuance of the NPCC guidance during Spring 2022, however these are still in draft status after several months. As Forces are transitioning to or are starting to utilise Komainu, they should ensure that these documents are equally updated for this change in process. However, during our audit we were not provided with any specific policies, procedures and/or guidance available to the Force/Unit for the handling of digital currency.
Risk	Inconsistent approaches to the seizure, storage and realisation of cryptocurrency.
Response	**Derbyshire** – Derbyshire Police follow the NPCC guidance on the seizure and retention of Crypto currency. Komainu are utilised as the custodian of any seizures. A Policy mirroring the NPCC guidance will be drafted later this year **Lincolnshire** – Lincolnshire Police already have a Procedure document in place, which parallels the NPCC guidance. All documents are available on the Team Lincolnshire Academy Intranet Page, along with the NPCC guidance videos. **Lincolnshire** – Lincolnshire Police acknowledge that we do not currently have a policy in place for the seizure of Crypto currency and we will be addressing that this year. We are a force with limited knowledge across the board but with recent training hopefully this has widened this skill set. We have recently updated our contract with Komainu..

Collaboration – Digital Currency 2022/23 (Continued)

Response	**Lincolnshire** - Procedure is live on our Policy/Procedure Library and has been signed off by DSupt PISCOPO. **EMSOU** – is addressing the lack of signed -off policy.
Responsibility / Timescale	**Derbyshire** DS Steve Judge October 2023 **Lincolnshire** DS Lee Taylor Completed **Lincolnshire** T/DS Richard Lister December 2023 **Lincolnshire** DS Thomas Curlett-New Completed **EMSOU** T/DI Colin Ellis October 23

We have also raised one priory 3 recommendation of a housekeeping nature:

- The Force/Unit should determine if risks related to digital currency should be included on their risk register.

Management agreed with the recommendations and both had been completed by the time the final report had been issued.

Collaboration – Performance Management 2022/23

Overall Assurance Opinion	Satisfactory

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

Our audit considered the following risks relating to the area under review:

• The collaboration units do not have a governance framework for managing performance and therefore poor performance is not addressed

• Lack of performance targets/measures and therefore a lack of clarity on levels of performance

• The collaboration units do not produce performance information in a timely manner.

• The collaboration units are not producing performance reports so those charged with governance can carry out their responsibilities effectively.

• Where benchmarking data is available it is not utilised to demonstrate levels of performance

• Where underperformance is highlighted actions are not put in place to address this.

We have raised two Priority 2 recommendation, which is significant, the full details of the recommendation and management response are detailed below:

Recommendation 1 (Priority 2)	The Units should ensure that they have clear performance targets that align to their business plans/objectives.
Finding	At the most recent review by the Regional Performance Analyst in September 2022, it was noted that EMSOU required clearer SMART performance targets for how well the unit is performing against its objectives. For EMSLDH it was noted that the performance reporting currently carried out did not clearly align to the unit's business plan/strategy. For EMCHRS OHU, it was noted that current performance information does not relate to the unit's business plan and that clear SMART targets should be set to allow for effective monitoring and reporting. However, this would be dependent on a new case management system.
Risk	Lack of performance targets/measures and therefore a lack of clarity on levels of performance.
Response	EMSOU Performance Manager will expand an existing framework to include key performance questions which reflect EMSOU strategic priorities to give a more broader, qualitative view of performance which shows outcomes and impact rather than just outputs. The Regional Performance Analyst will be involved with this work to ensure it reflects PCC need. EMSLDH Response: Via the Regional L&D Management Board, EMSLDH have been requested to revise performance reporting in line with the recommendation made within this report, whereby performance will clearly align to EMSLDH Business Plan and Strategy and will be ratified at the next Regional L&D Management Board. In addition EMSLDH will revise activity tracking. These will be shared throughout the year with the PCC and CC Board. EMCHRS OHU- this collaboration disbanded as of end of FY 2022/23 so no longer appropriate to action.

Collaboration – Performance Management 2022/23 (Continued)

Recommendation 2 (Priority 2)	Benchmarking opportunities should be explored by the Units and the Regional Performance Analyst so that performance can be appropriately measured and compared.
Finding	Benchmarking is an important tool to allow organisations to measure themselves against similar comparators and identify best practice. However, due to limited data and opportunities, the only benchmarking carried out is by EMSOU using NFIB data to compare themselves against other ROCUs. Audit has noted that there are programmes underway to try and develop benchmarking, such as the National Strategic Performance Framework, however these opportunities are not yet well developed.
Risk	Units are not aware of their performance and are not able to identify best practice.
Response	Benchmarking between ROCU's is a known difficulty due to differences in recording practices and ROCU frameworks. As highlighted, there is national work ongoing around improving the ability to benchmark between ROCU's and other capabilities. EMSOU and the Regional Performance Analyst will continue to monitor this work with expectations of embedding in practice when national work completed. There is some benchmarking and highlighting of best practice currently through the ROCU Executive Performance report; the Regional Performance Analyst will work with the EMSOU Performance Manager to ensure that PCC's are appropriately sighted on existing activity.
Responsibility / Timescale	Sept 2023

Section 04 - Statement of Responsibility

We take responsibility to Lincolnshire Police and the Officer of the Police & Crime Commissioner (OPCC) 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.