

<b>For Information / Consideration</b>	
<b>Public/Non Public*</b>	<b>Public</b>
<b>Report to:</b>	<b>Joint Audit and Scrutiny Panel</b>
<b>Date of Meeting:</b>	<b>23<sup>rd</sup> September 2014</b>
<b>Report of:</b>	<b>Chief Finance Officer</b>
<b>Report Author:</b>	<b>Charlotte Radford</b>
<b>E-mail:</b>	
<b>Other Contacts:</b>	<b>Angela Ward</b>
<b>Agenda Item:</b>	<b>8</b>

## **INTERNAL AUDIT PROGRESS REPORT**

### **1. Purpose of the Report**

- 1.1 To provide members with an update on progress against the Internal Audit Annual Plan and the findings from audits completed to date.

### **2. Recommendations**

- 2.1 Members are recommended to consider the report and where appropriate make comment or request further work in relation to specific audits to ensure they have adequate assurance from the work undertaken.

### **3. Reasons for Recommendations**

- 3.1 This complies with good governance and in ensuring assurance can be obtained from the work carried out.

### **4. Summary of Key Points**

- 4.1 The attached report details the work undertaken to date and summarises the findings from individual audits completed since the last progress report to the panel.

### **5. Financial Implications and Budget Provision**

- 5.1 None as a direct result of this report.

### **6. Human Resources Implications**

- 6.1 None as a direct result of this report.

### **7. Equality Implications**

- 7.1 None as a direct result of this report.

## **8. Risk Management**

8.1 None as a direct result of this report.

## **9. Policy Implications and links to the Police and Crime Plan Priorities**

9.1 This report complies with good governance and financial regulations.

## **10. Changes in Legislation or other Legal Considerations**

10.1 None

## **11. Details of outcome of consultation**

11.1 Not applicable

## **12. Appendices**

12.1 Appendix A - Internal Audit progress report.

# **Nottinghamshire Office of the Police & Crime Commissioner & Nottinghamshire Chief Constable**

## **Internal Audit Progress Report**

Audit Committee meeting: 23<sup>rd</sup> September 2014

## Introduction

The internal audit plan for 2014/15 was approved by the Joint Audit & Scrutiny Panel in June 2014. This report provides an update on progress against that plan and summarises the results of our work to date.

### Summary of Progress against the Internal Audit Plan

The table below provides a progress summary of the reports that have been finalised, in draft or are work in progress. There are no fundamental issues to report to the Committee that may impact on our annual Head of Internal Audit opinion at this time.

Assignment <i>Reports considered today are shown in italics</i>	Status	Opinion	Actions Agreed (by priority)		
			High	Medium	Low
Audits to address specific risks					
<i>Information Management Arrangements</i>	<i>Final Report</i>	<i>Advisory</i>	-	8	2
<i>Information Security – Disaster Recovery</i>	<i>Final Report</i>	<i>Amber/Green</i>	-	2	3
Commissioning	Q4				
Governance – Delivery of Police & Crime Plan	In the process of being scoped				
Partnerships	Q3				
Policy Review	As and When				
Scrutiny Panel	Q3				
Crime Recording Follow Up	Q4				
Volunteering	In the process of being scoped				
Regional HR – Training & Skills	Refer to comments included in the Change Control section				
Victims Code of Compliance	In the process of being scoped				
Key Financial Controls	Q3				
Forensics Support Scientific Support	Q2				
Financial Regulations	Q2				
Corporate Governance / Policy Making	Q4				
Follow Up	Q4				
Regional Review	The scope has been agreed				

## Other Matters

### Planning and Liaison:

We have continued to regularly meet and liaise with key officers and have also held various planning meetings with management to discuss the specific scoping of individual reviews and to agree the proposed timings of these reviews.

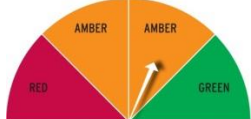
### Internal Audit Plan 2013/14 - Change Control:

Action	Date	Agreed By
<i>Changes considered today are shown in italics</i>		
<i>The regional HR Training &amp; Skills audit has been requested to be deferred until 2015/16. However, it is intended to utilise the allocation for this review to complete the regional review (with Northamptonshire Police) on Microsoft Licensing.</i>	<i>September 2014</i>	<i>To be agreed by the Joint Audit &amp; Scrutiny Panel – September 2014</i>

**Information and Briefings:** We have issued the following updates electronically since the last Joint Audit & Scrutiny Panel:

- Emergency Services News Briefing - August 2014

## Key Findings from Internal Audit Work

<b>Assignment: Business Continuity &amp; IT Disaster Recovery Planning</b>	<b>Opinion: Amber / Green</b>	
<p>The Force is currently in a period of transition moving a number of its virtual servers into a cloud based solution. Furthermore, the personnel within IT has changed during 2014 with the Infrastructure and Service Delivery Manager taking on responsibility for IT business continuity. Support and guidance for Force-wide Business Continuity is provided by the Strategic Support Officer.</p> <p>The Force is driven by ACPO guidelines to determine the criticality of IT systems and services for response times. The main IT operating site is at Police Head Quarters in Nottingham, with a failover site located within the county at Mansfield and a third smaller site is available for IT disaster recovery and continuity at Carlton Police Station.</p> <p>The key findings from this review are as follows:</p> <p><b>Design of control framework</b></p> <ul style="list-style-type: none"> <li>▪ The Force has a combination of physical servers, a virtualised platform and a cloud platform. All business continuity data is backed up according to a documented schedule to a backup server which is housed at Force Headquarters in Nottingham.</li> <li>▪ The Force has two data centres facilitating the continuity of data - Force Headquarters which is the backup site and Mansfield Police Station which is the recovery site. A further smaller recovery site is sited at Carlton Police Station within the County.</li> <li>▪ These three core sites are triangulated in their configuration so if a link fails at any one site the others will remain operable; we verified this by review of a network diagram showing that it was last updated January 2014.</li> <li>▪ The IT department has an Excel document which shows what servers are backed up, the frequency and the storage location to failover site. There is also a data domain backup document which covers how backups are performed. A Legato Data Domain Backup System is used by the IT department to manage and review backups; this is referred to as DDR.</li> <li>▪ The backup system in place is designed to enable the IT Operations Team to monitor backup success, incidents and failures on a daily basis via the system management console; this ensures they are completed in accordance with the schedule.</li> <li>▪ A Formal Business Impact Analysis has been undertaken and is documented in the Force's IT Business Continuity Toolkit which is maintained and retained on the Operations J Drive on the Force's network. The Business Impact Analysis shows interruption exposures to the IT systems and services, their probability and impact and remediation alternatives.</li> <li>▪ To ensure that staff are aware of their responsibilities in the event of a disaster, responsibility for IT Business Continuity has been assigned to appropriate members of staff and a Crisis Management Team have been defined.</li> <li>▪ An uninterrupted power supply (UPS), which is used to supply a safe power supply should there be a loss of main power is in place and is powered by a generator at the three core sites. The time available is dependent on the current server load which was showing as 78 minutes during our review.</li> <li>▪ To ensure that IT hardware is available and would be replaced should an issue occur there are a number of contracts in place with 3<sup>rd</sup> party suppliers. The scope and remit of this cover was found to be satisfactory.</li> <li>▪ An adequate service level management control framework for the provision of hardware, telephony and airwave services is in place and is designed to ensure that third party arrangements exist to maintain the continuity of IT services.</li> <li>▪ To ensure appropriate finance would be available in the event of a disaster the Force also has computer insurance with Tokio Marine London for the period 1st May 2014 to 30<sup>th</sup> April 2015 which includes schedules for computer and business interruption.</li> </ul> <p><b>Application of and compliance with control framework</b></p> <ul style="list-style-type: none"> <li>▪ We reviewed the DDR backup console for one day during our fieldwork to confirm that live daily</li> </ul>		

backups and network monitoring using Solarwinds were occurring at the Force's backup site in accordance with documented procedures. We found these to be operating without any continuity issues at the time of review.

- Monthly failover testing of the Force control room system "Vision" is conducted. We obtained and reviewed the log of these monthly tests for the previous six months and can confirm that these were carried out satisfactorily and any issues with the equipment were reported and logged for resolution rendering the system fit for purpose.

However, we have made two medium category and three low category recommendations to assist the Force with its IT Business Continuity Planning. The medium rated findings and recommendations are summarised below:

- The IT Department has recently developed an IT Business Continuity Toolkit which contains a suite of related documents and is aligned to ISO 22301. The document is not yet fully complete. In addition associated key recovery documentation for each of the IT services held separately within the Business Continuity Folder on the network is also not complete and has not been formally reviewed as appropriate and approved by senior management (this will be updated as part of the IT Business Continuity Toolkit documentation). Therefore there is an increased risk if relevant required guidance and information is not available in a disaster event, which could lead to a delay or inability to restore key IT services across the Force within an acceptable timeframe.
- The Business Continuity Plan is currently only tested using "desktop" Force wide exercises. It has yet to be tested for IT failure scenarios and results recorded; a full periodic test at the disaster recovery site is yet to be scheduled and undertaken and our review of the documentation provided and discussions with IT Management confirmed that they do not currently perform restoration testing of servers containing critical IT services from backup data. Currently without comprehensive testing there is limited assurance that the Force is able to recover critical systems and data within an acceptable recovery time should a disaster occur.

Recommendation	Management Action	Responsible Officer / Date
An action plan needs to be developed to ensure IT Information Services have a complete and up to date Business Continuity Toolkit and associated suite of recovery documentation covering all the identified critical IT services. (Medium)		
Job descriptions need to be aligned to the IT Business Continuity Toolkit and updated to include responsibilities for IT Business Continuity, particularly for those in the Crisis Management Team. (Low)		
The Business Continuity Toolkit and other supporting documentation held in the directory to assist recovery in the event of a disaster occurring should be completed and stored securely offsite; in addition to the backup so available immediately should a disaster occur. (Low)		
The IT Business Continuity Toolkit - Tests & Exercise Tab should be fully completed and should provide comprehensive details of testing planned and undertaken. (Low)		
An IT Business Continuity test schedule should be documented and approved. The IT Business Continuity Toolkit should be		

tested at least annually or after a change of key personnel, operational system or any aspect of the operational infrastructure. Where recovery testing takes place this should also assess recovery point and recovery time testing to ensure the specified objectives are achieved. (Medium)		
---	--	--

Assignment: Information Management Arrangements (01.14/15)	Opinion:	Advisory
<p>Headline Findings:</p> <p>Introduction</p> <p>Nottinghamshire Police (the Force) has recently completed a MoPI (Management of Police Information) questionnaire. On the back of the submitted responses HMIC (Her Majesty's Inspectorate of Constabulary) has issued an inspection letter covering a number of key areas. The inspection is due to be completed in June 2014. As part of the Force's Information Assurance Framework they have an established Force Information Assurance Board (FIAB) which meets quarterly and has a standardised agenda. To assist the FIAB the Force have recently established an Information Risk Management Group (IRMG) which will have their first meeting in May 2014 and monthly moving forward. This working group will feed into FIAB.</p> <p>The Deputy Chief Constable (DCC) is the Force's Association of Chief Police Officers (ACPO) lead on information assurance, information sharing agreements and also the Force's nominated SIRO. She chairs FIAB and is part of IRMG.</p> <p>A number of areas of adequately designed and controls were identified during the review, including the following:</p> <p><b>Design of control framework</b></p> <ul style="list-style-type: none"> <li>▪ To ensure that responsibilities are clear, Information Asset Owner (IAO) responsibilities have been documented within the Information Assurance Framework (IAF) and initial workshops have been undertaken with those staff whose role includes being an IAO;</li> <li>▪ To develop the Force's information management control framework and to provide evidence to the HMIC inspectors that improvements are being made the Force has documented a draft Information Assurance Improvement Plan (IAIP); and</li> <li>▪ To ensure records are retained in accordance with agreed guidelines a retention schedule has been documented this includes the retention periods for key Force records.</li> </ul> <p>However, we have made eight medium recommendations in relation to the design of the control framework. The findings are summarised below:</p> <ul style="list-style-type: none"> <li>▪ The MoPI Questionnaire submission for 2013 was not subject to approval by an appropriate group or committee to ensure that answers were a fair representation of the Force's information management arrangements;</li> <li>▪ The Force does not have a full suite of up to date and documented information management policies and associated procedures. Without appropriate policies and procedures the Force is increasing the risk that staff are not aware of their responsibilities which could lead to the incorrect handling of sensitive information;</li> <li>▪ Information Assurance training is a mandatory module for all staff; however this does not include the MoPI training. Accordingly, the Force are not able to submit this as complete on the questionnaire;</li> <li>▪ The Force has a number of information sharing agreements (ISAs) in place with third parties. There is a comprehensive centralised repository which is used to identify information that flows in and out of the Force. Although there is a list which shows current and withdrawn ISA's which Management advised is reviewed annually some gaps were showing at the time of our review and therefore assurance is reduced over the validity of the ISAs within the list;</li> <li>▪ A data flow mapping exercise to identify inbound and outbound personal and sensitive</li> </ul>		

<p>information flows within and outside the Force has not been performed. This would allow the Force to review whether secure transportation of sensitive information is being performed;</p> <ul style="list-style-type: none"> <li>▪ Quality assurance audits of information held and intelligence captured to ensure that information is recorded accurately and effectively are not scheduled or undertaken;</li> <li>▪ MoPI groupings used for categorising nominal crimes (as required by MoPI) are not utilised within the Force's crime data; and</li> <li>▪ The Force does not currently have a comprehensive Information Assurance Risk Register we would expect this to be linked to an Information Assurance Improvement Plan (IAIP) with a prioritisation given to each improvement action. A risk register is used to identify all current information risks and to document mitigating controls so that risks can be effectively managed.</li> </ul>		
Recommendation	Management Action	Responsible Officer / Date
<p>To ensure that external facing communication is both accurate and approved at a senior level further questionnaires (not just MoPI) should be discussed and approved once completed and before being sent to a third party.</p> <p>Ideally the FIAB should be responsible for collating and approving responses to information assurance questionnaires and ultimate authorisation should be from the SIRO. (Medium)</p>	<p>The business areas which deal with the questionnaire were consulted. Each section was completed by a specialist in post. FIAB only meet once a quarter so the timescales were not conducive to the 3 week turnaround requested of the questionnaire. All future questionnaires will be the responsibility (within reason) of the SIRO and approval through FIAB. As FIAB only meets quarterly it is not always practicable to approve through FIAB therefore, where appropriate, approvals will be sought through the monthly IRMG meetings or via the Interim Information Management and Security Manager or the Organisational Development Manager direct to the SIRO</p>	<p>SIRO</p> <p>Implemented</p>
<p>To ensure that responsibilities and procedures are clear, the Force needs to develop and implement a comprehensive Information Management Strategy in line with national guidance. (Medium)</p> <p>To support the Information Management Strategy the Force should complete the following actions:</p> <ul style="list-style-type: none"> <li>• To ensure that staff are fully aware of their individual responsibilities a comprehensive range of policies and procedures which should include but not be limited to records management, information security, data disposals and data quality that are associated with the Information Management Strategy should be documented, approved and implemented to support the Strategy.</li> <li>• To ensure the consequences of a lack of formal documentation is understood by</li> </ul>	<p>Carry out a comprehensive review of information management responsibilities, to enable us to identify the extent to which we currently meet information management responsibilities, along with identification of any risks which are likely to impact on those responsibilities in the future.</p> <p>This recommendation only partly relates to risk management.</p> <p>College of Policing APP on Information Management</p>	<p>Pat Stocker (Information Security Manager)</p> <p>31/8/14</p>

<p>senior management the Force should ensure that the Information Assurance Improvement Plan and Risk Register is updated to include the risks and implications of not having in place appropriate Strategies and Policies.</p> <p>So that policies and procedures are relevant and progress of the implementation of the Strategy and associated policies and procedures should be monitored by the IRMG and FIAB. (Medium)</p>	<p>states a strategy is required. Evidence gathered will inform the nature of the Strategy.</p>	
<p>To ensure that staff are fully aware of their individual responsibilities the Force should ensure the following actions are undertaken:</p> <ul style="list-style-type: none"> <li>• All staff should undertake mandatory Information Management Training as per the Information Assurance Framework.</li> <li>• Training records should be formally reported to FIAB in order to measure compliance.</li> <li>• A Training Needs Analysis should be performed and executed to identify those staff with elevated information management responsibilities, e.g. IAOs to ensure further relevant training modules like MoPI are made mandatory.</li> <li>• Consideration should be given to implementing periodic mandatory information management refresher training.</li> </ul> <p>(Medium)</p>	<p>Commission training at regional level at the regional IA Board chaired by the SIRO and deliver e-learning packages for all staff.</p> <p>Review the training delivery via the Training Priorities Panel chaired by the Force SIRO</p>	<p>Pat Stocker (Information Security Manager) 31/12/14</p>
<p>The Force should ensure that all ISAs are documented within a comprehensive centralised repository to confirm that appropriate agreements are in place.</p> <p>In addition, once completed, the centralised repository should be reviewed periodically to ensure that the agreements are up to date, are still required and are adhered to. (Medium)</p>	<p>Review all the ISA's to ensure fit for purpose and place in the NC Forms network folder so accessible to all staff.</p>	<p>Pat Stocker (Information Security Manager)  31/12/14</p>
<p>The Force should perform a data flow mapping exercise to identify information flows within and information that leaves and enters the organisation. (Low)</p>	<p>Carry out a data flow mapping exercise to identify information that leaves and enters the organisation.</p>	<p>Pat Stocker (Information Security Manager) Phased approach with full completion due by 31<sup>st</sup> March 2015</p>
<ul style="list-style-type: none"> <li>• To ensure that assurance can be gained that staff are following the appropriate procedures and data quality is an appropriate standard the Force should look to complete the following actions:</li> <li>• Implement a comprehensive information quality assurance audit programme which is in accordance with an agreed Information Management Strategy.</li> <li>• An Audit Schedule and a standardised</li> </ul>	<p>Carry out a comprehensive review of information management responsibilities (as per 1.2)</p> <p>Review the quality assurance audit programme to ensure in line with the Information Management Strategy.</p>	<p>Pat Stocker (Information Security Manager)  31/08/2014  31/08/2014</p>

<p>programme test template should be agreed which covers but is not limited to a sample assessments of data transfers and information sharing agreements</p> <ul style="list-style-type: none"> <li>Results of all audits should be reported to FIAB.</li> </ul> <p>(Medium)</p>	<p>In the proposed restructure it is thought the post of Information Sharing Officer will include the responsibility for audit of information sharing. Refresh the audit schedule and present to FIAB.</p>	
<p>The Force should implement MoPI groupings so that nominal crimes can be clearly grouped and reviewed. (Medium)</p>	<p>Implement a system which will allow the grouping and review of nominals or crimes.</p> <p>Review current status of MOPI classifications within the current MOPI systems and review technical and business process options available alongside the current Force priorities to assess how this recommendation can be achieved</p>	<p>Pat Stocker (Information Security Manager)</p> <p>Phased approach with completion by 31<sup>st</sup> March 2015</p>
<p>To ensure that the Force is fully aware of the consequences of any risks in place and to ensure that appropriate mitigating actions are taken/agreed an Information Assurance Risk Register should be completed and reviewed formally at the FIAB and (IRMG).</p> <p>The Risk Register should be linked and referenced to the Information Assurance Improvement Action Plan and the prioritisation of each action should be listed. (Medium)</p>	<p>An Information Risk Strategy and Risk Register are in development; terms of reference for the IRMG have been agreed by the DCC and monthly meetings set up to formally review development of the Information Risk Register alongside the required business processes with progress reported to FIAB.</p>	<p>Pat Stocker (Information Security Manager)</p> <p>Implemented</p>
<p>To ensure that actions will be completed in a timely manner the Information Assurance Improvement Plan should be updated and reviewed in light of breached completion dates. (Low)</p>	<p>Regularly review and update the Information Assurance Improvement Plan</p>	<p>Pat Stocker (Information Security Manager)</p> <p>Ongoing</p>

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information provided in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regard to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

This report, together with any attachments, is provided pursuant to the terms of our engagement. The use of the report is solely for internal purposes by the management and Board of our client and, pursuant to the terms of the engagement, it should not be copied or disclosed to any third party or otherwise quoted or referred to, in whole in part, without our written consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose.

© 2013 Baker Tilly Business Services Limited

The term "partner" is a title for senior employees, none of whom provide any services on their own behalf.

Baker Tilly Business Services Limited (04066924) is registered in England and Wales. Registered office 25 Farringdon Street, London, EC4A 4AB.