

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

Internal Audit Progress Report

Audit Committee meeting: December 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 | | | | | |
| Information Management Arrangements | Final Report | Advisory | - | 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 | Fieldwork planned to commence 12/01/2015 | | | | |
| Partnerships | Fieldwork planned to commence 02/03/2015 | | | | |
| Policy Review | As and When | | | | |
| Scrutiny Panel | Fieldwork planned to commence 16/02/2015 | | | | |
| Crime Recording Follow Up | Q4 | | | | |
| Volunteering | Draft Report issued | | | | |
| Regional HR – Training & Skills | Refer to comments included in the Change Control section | | | | |
| Victims Code of Compliance | Fieldwork planned to commence 05/01/2015 | | | | |
| Key Financial Controls | Draft Report issued | | | | |

| | | | | | |
|--------------------------------------|--|--|--|--|--|
| Forensics Support Scientific Support | Refer to comments included in the Change Control section | | | | |
| Financial Regulations | Refer to comments included in the Change Control section | | | | |
| Corporate Governance / Policy Making | Refer to comments included in the Change Control section | | | | |
| Follow Up | Q4 | | | | |
| Regional Review | The scope has been agreed | | | | |

Other Matters

Planning and Liaison: We have met with management to discuss the progress of the 2014/15 audit plan.

In addition, we held a Joint East Midlands Chief Finance Officers (OPCC & Force) workshop to discuss collaborative assurances and how these can be effectively achieved and how Internal Audit can feed into this process.

Since the last meeting, following discussion at the East Midlands Joint Chief Finance Officers meeting it was agreed that we would undertake an additional review of G4S Niche Service Provision through Lincolnshire Police to be able to provide assurance to the region on the arrangements in place. The results of this audit are included in this progress report for information, but have been scrutinised at Lincolnshire Committee.

Internal Audit Plan 2014/15 - Change Control:

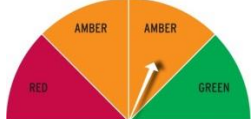
| Action <i>Changes considered today are shown in italics</i> | Date | Agreed By |
|--|----------------------|---|
| The regional HR Training & Skills audit has been requested to be deferred until 2015/16. However, it is intended to utilise the allocation for this review to complete the regional review (with Northamptonshire Police) on System Licensing. | September 2014 | To be agreed by the Joint Audit & Scrutiny Panel – September 2014 |
| <i>We had an allocation for Financial Regulations & Corporate Governance, but this has not been required. Instead, the allocation will be utilised to complete regional work around the Assurance Framework for Collaborations.</i> | <i>December 2014</i> | <i>To be agreed by the Joint Audit & Scrutiny Panel – December 2014</i> |
| <i>We had an allocation for Forensics – Scientific Support, but this has not been required. Instead, the allocation will be utilised to complete some audit work around grants and grant allocations within Force.</i> | <i>December 2014</i> | <i>To be agreed by the Joint Audit & Scrutiny Panel – December 2014</i> |

Information and Briefings:

We have issued the following updates since the last Committee:

- Emergency Services News Briefing – October 2014
 - Code of Ethics: A Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales.
 - Fire Incidents Response Times: England, 2013-14.
 - Revised PACE Code A.
 - Core business: An inspection into crime prevention, police attendance and the use of police time.
 - A master class in managing contracts and getting best value from third party providers.
 - New National Fraud Initiative Security Policy Compliance Declaration.

Key Findings from Internal Audit Work

| | | |
|--|-------------------------------|---|
| Assignment: Business Continuity & IT Disaster Recovery Planning | Opinion: Amber / Green |  |
| <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>Design of control framework</p> <ul style="list-style-type: none"> ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ 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. ▪ To ensure that IT hardware is available and would be replaced should an issue occur there are a number of contracts in place with 3rd party suppliers. The scope and remit of this cover was found to be satisfactory. ▪ 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. ▪ 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 30th April 2015 which includes schedules for computer and business interruption. | | |

Application of and compliance with control framework

- We reviewed the DDR backup console for one day during our fieldwork to confirm that live daily 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) | This is already work in progress, Action: Update the Information Services department Business Continuity Plan using the Force BC Toolkit. Action: Create a suite of recovery documentation covering all identified critical IT systems. | Julie Mansfield 31 Dec 2014 |
| 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) | Responsibilities for business continuity and crisis management are contained within the Force BC Policy and Strategy; to include specific reference to this in individual job descriptions would be overly bureaucratic and add no value. | N/A |

| | | |
|--|--|--------------------------------|
| 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) | Implemented | Julie Mansfield Implemented |
| The IT Business Continuity Toolkit - Tests & Exercise Tab should be fully completed and should provide comprehensive details of testing planned and undertaken. (Low) | Update the Information Services department Business Continuity Toolkit Test & Exercise record with the results of Exercise Candle and the date of next year's test | Julie Mansfield 31 Dec 2014 |
| 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) | This approach is becoming normal for new systems and as confidence grows this can form part of a planned approach and performed during the pre-planned maintenance windows. Action: Plan, document and gain approval from the head of department for an Information Services disaster recovery test schedule and record; tests should be at least annually and after any changes to key personnel, operational system or infrastructure. | Julie Mansfield 31 Dec 2014 |

| Lincolnshire Police - G4S Niche Service Provision (for information only) | Opinion: Green | Substantial Assurance |
|--|---------------------------|------------------------------|
| <p>Introduction</p> <p>Niche RMS (hereafter referred to as Niche) is a single, unified, operational policing system that manages information in relation to the core policing entities – people, locations, vehicles, organisations, incidents and property.</p> <p>Niche was implemented by Lincolnshire Police Force (hereafter referred to as Lincolnshire) in January 2010 and the system was identified as having the potential of becoming the spinal infrastructure for policing information going forward.</p> <p>G4S Care and Justice Services (UK) Limited were contracted to deliver various services incorporating ICT (including Niche), in April 2012 and following extensive work, the Chief Constables and Police & Crime Commissioners for Lincolnshire, Leicestershire, Northamptonshire and Nottinghamshire forces agreed to move to a single instance of Niche for crime, intelligence, case, custody and associated information databases.</p> <p>The preferred method for achieving this is for Leicestershire, Northamptonshire and Nottinghamshire to enter into a formal collaboration agreement with Lincolnshire, and for Lincolnshire to provide the Niche hosting service.</p> | | |

Leicestershire, Nottinghamshire and Northamptonshire will therefore be reliant upon Lincolnshire and its G4S contractors for the provision of essential operational IT services for a period of at least three years. Accordingly, the relevant Chief Constables and Police & Crimes Commissioners wished to secure assurance of G4S's performance delivery regarding services provided to Lincolnshire in respect of Niche.

Conclusion

Based on the work undertaken as part of this review, Lincolnshire can take substantial assurance that the control framework and infrastructure that are currently in place allow for the effective facilitation, management and governance of the G4S Niche service provision. The control framework is supported by effective communication and a strong working relationship that will help to ensure processes remain robust and reflective of developing arrangements as Niche is driven forward and rolled out across the other forces in the East Midlands region.

The scope of the review and indeed our conclusion has focused upon the governance framework and management of the existing G4S contractual arrangements. There are other areas that will need deliberation once the project is in its implementation stage that the individual Forces will need to consider and manage and these areas are around the cleansing of data within the individual force systems and the accuracy of this, prior to it being transferred to any new system and indeed the ownership of such data once it is transferred.

As a practising member firm of the Institute of Chartered Accountants in England and Wales (ICAEW), we are subject to its ethical and other professional requirements which are detailed at <http://www.icaew.com/en/members/regulations-standards-and-guidance>.

The matters raised in this report are only those which came to our attention during the course of our review 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. This report, or our work, should not be taken as a substitute for management's responsibilities for the application of sound commercial practices. We emphasise that the responsibility for a sound system of internal controls rests with management and our work should not be relied upon to identify all strengths and weaknesses that may exist. Neither should our work be relied upon to identify all circumstances of fraud and irregularity should there be any.

This report is supplied on the understanding that it is solely for the use of the persons to whom it is addressed and for the purposes set out herein. Our work has been undertaken solely to prepare this report and state those matters that we have agreed to state to them. This report should not therefore be regarded as suitable to be used or relied on by any other party wishing to acquire any rights from Baker Tilly Risk Advisory Services LLP for any purpose or in any context. Any party other than the Board which obtains access to this report or a copy and chooses to rely on this report (or any part of it) will do so at its own risk. To the fullest extent permitted by law, Baker Tilly Risk Advisory Services LLP will accept no responsibility or liability in respect of this report to any other party and shall not be liable for any loss, damage or expense of whatsoever nature which is caused by any person's reliance on representations in this report.

This report is released to our Client on the basis that it shall not be copied, referred to or disclosed, in whole or in part (save as otherwise permitted by agreed written terms), without our prior written consent.

We have no responsibility to update this report for events and circumstances occurring after the date of this report.

Baker Tilly Risk Advisory Services LLP is a limited liability partnership registered in England and Wales no. OC389499 at 6th floor, 25 Farringdon Street, London EC4A 4AB.

© 2013 Baker Tilly Risk Advisory Services LLP.