Internal Audit

Progress Report

Newark and Sherwood District Council – October 2018

Assurance LINCOLNSHIRE
For all your assurance needs

NEWARK & SHERWOOD DISTRICT COUNCIL

Contents

Lucy Pledge - Audit and Risk Manager (Head of Internal Audit)
lucy.pledge@lincolnshire.gov.uk

John Sketchley – Audit Team Leader
John.sketchley@lincolnshire.gov.uk

Amanda Hunt - Principal
Amanda.hunt@newark-sherwooddc.gov.uk

Introduction

The purpose of this report is to:

Provide details of the audit work during the period April 2018 to October 2018
Advise on progress with the 2018/19 plan
Raise any other matters that may be relevant to the Audit Committee role

Key Messages

During the period we have completed 9 audits:

- 7 to final assurance reports
- 2 other reports - Consultancy

Assurances

The following audit work has been completed and a final report issued:

- ICT – PCIDSS - Limited
- IR35 (Intermediaries Legislation) - Substantial
- S106 – Substantial
- Risk Management - Substantial
- Active4Today Creditors - Substantial
- Key Controls - Substantial
- ICT – Meritec System – Substantial

Consultancy

The following consultancy work has been completed:-

- Corporate Policy
- Contract Management

Note: The assurance expressed is at the time of issue of the report but before the full implementation of the agreed management action plan. The definitions for each level are shown in Appendix 1.

0
HIGH ASSURANCE

6
SUBSTANTIAL ASSURANCE

1
LIMITED ASSURANCE

0
LOW ASSURANCE

Limited Assurance

PCIDSS

The Council has not progressed the required documentation and evidence to support the annual PCI DSS compliance assessment. As a result the Council is not PCI DSS compliant and we can only give a limited assurance opinion at this time.

Additional pressures have been experienced with the Council relocating its premises, which diverted a lot of IT resources, notably those of the Assistant IT Manager who led on PCI DSS compliance. Shortly thereafter the Assistant IT Manager then left the Council. This position has not been filled, although PCI DSS compliance has now been picked up by a member of staff within the IT section.

The Council may have access, through its acquiring bank, to an online portal that could help with the PCI DSS compliance process. We have raised this matter with both the IT and Finance teams and have made a recommendation to determine whether this online portal is available to the Council as this would likely greatly simplify compliance work.

Our recommendations from the previous audit review, undertaken in May 2016, are largely restated with requirements to:-

- Confirming the availability of an online portal with the acquiring bank to assist PCI DSS compliance. If this is not available, then annual formal project arrangements are put in place to ensure a staged approach to compliance is undertaken.

- Annually identify and document all of the system components within the Council that interact with cardholder data. Determining this scope is foundational to complying with PCI DSS. Without a clear understanding of scope, the Council cannot validate its boundaries and would not know where to apply the requirements.

- Complete the relevant self-assessment questionnaire (SAQ). The SAQ is designed as a self-validation tool to assess security for cardholder data. The Self-Assessment Questionnaire includes a series of yes-or-no questions. If an answer is "no", the Council may be required to state the future remediation date and associated actions to resolve to a "yes".

Management Comments

- ICT accept the recommendations included within the report and will give appropriate focus and commitment to addressing the issues to complete the compliance.

Substantial Assurance

IR35

Overall, the arrangements in place ensure that the IR35 regulations are complied with and management continue to explore and implement measures that will enhance full compliance. Our assurance is supported through a number of areas of good practice including:-

- Policy and brief guidance notes are in place
- HMRC's online toolkit is used to check the employment status of the workers or contractors engaged.
- Intermediaries are notified the outcomes of the employment status checks.
- HR keeps a register of IR35 engagements across the Council and ensures ongoing dialogue with the Business Managers.

Currently there are no engagements on the IR35 register which have been assessed as employees of the Council that require the collection and submission of the related tax and NICs to HMRC.

An ongoing review of the employment status for new and existing Personal Service Companies within each Business Unit and reporting the outcomes promptly to HR would ensure that an accurate and complete IR35 register is maintained and enhance the assurance arrangement.

S106

Overall, the processes in place for managing S106 income collection and expenditure are operating sufficiently ensuring effective management of the activity and continual development. The funds are used in accordance with the agreements. This is supported through a number of areas of good practice including:-

- Ongoing monitoring of the triggers to enable invoicing
- Monitoring of the receipts and expenditure for each scheme
- Senior Management oversight of the
- Receipts and expenditure accurately recorded within the General Ledger
- Close working relationship between the Infrastructure and S106 Officer and the Assistant Accountant
- Formal S106 agreements for the identified development activities

Areas where some improvements are necessary include:-

- Provision of reports to the relevant committees presenting financial and activity performance.
- Accurate recording of the trigger information on the database.
- Retention of the indices used for the calculation of inflation

We have provided substantial assurance on the arrangements as most aspects are managed well. However, it is borderline limited as we identified several areas where significant improvements are necessary to strengthen safe working environments.

Substantial Assurance

Risk Management

Overall, the Risk Management arrangement is adequately managed and the related processes currently in place are operating effectively to reduce the impact of the risk. This is supported through a number of areas of good practice including:-

- Established and well attended Risk Management Group
- Corporate Management Team (CMT) involvement in the risk workshops setting the tone from the top
- Established risk registers
- Risks are considered when developing key policies and in decision making
- Knowledgeable staff

We identified some areas where improvements are necessary to enhance the controls, including:-

- Producing regular risk management reports for the Audit and Accounts Committee to support their oversight role
- Establishing a risk maturity target level
- Ensuring involvement of appropriate committees when reviewing and approving the Risk Management Strategy
- Reviewing responsibilities within the risk management policy to ensure they are clearly defined
- Timely review of the risk registers, completion of the risk assessments and risk actions
- Incorporating risks associated with the Council's subsidiary companies, partnerships and joint working arrangements within the risk registers.
- Reviewing the resources allocated for the risk management functions

Active4 Today Creditors

The systems and processes put in place will ensure that creditors are processed and paid correctly. There are several authorisation and checking processes which ensure that invoices are entered fully and paid. Areas of good practice include:-

- System restrictions in place enforcing separation of duties
- Management checking throughout the various processes
- Knowledgeable and experienced staff
- Documentation maintained supporting the payments and authorisation processes

We did identify some areas where improvements are required. These include:-

- Reviewing access to the financial system and ensuring that any changes are authorised
- Amending the batch control header sheet to record accountability and include explanation of differences
- Checking of the payment batch file, particularly high values
- Ensuring the security of the BACS download file

Substantial Assurance

Key Controls

The Council has good processes and sufficient key controls in place which ensure that the financial systems reviewed operate effectively protecting the business from increased exposure to fraud and error. We have identified some areas where further improvements are necessary:-

Creditors

- Amendments to the creditor's bank account details are authenticated or confirmed before any payment is made.

Debtors

- Formalising the arrangements when setting up debtor accounts and maintaining a record of any supporting documentation
- Establishing a sundry debtors collection target
- Ensuring correct balance for Trade Waste debtors is held in the General Ledger
- Accurately updating write-offs on the General Ledger.

Payroll

- Ensuring the authorised signatories send the accompanying emails supporting the digitally signed documents and both are retained.

Treasury Management

- Regularly reviewing and updating the Treasury Management manual

Council Tax and NNDR

- Ensuring the number of Council Tax and NNDR bills printed and despatched are reconciled to those expected by the Council and discrepancies identified are corrected.

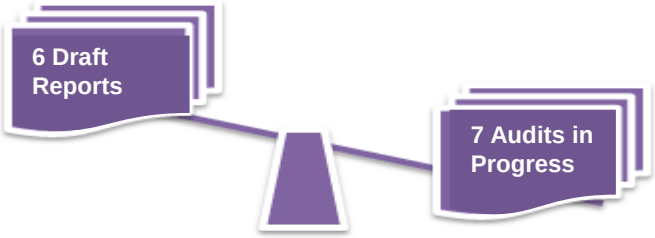
ICT Meritec System

The Council's relationship with Meritec and the development of systems on its ESB platform is an on-going and developing one. Our assessment of the Council's development of applications on the Meritec ESB platform is that there is a substantial level of assurance that the use of Meritec has resulted, and will continue to result, in improved service delivery arrangements in line with the Council's Digital Strategy. Key areas supporting this include:-

- Effective management involvement and oversight of the development of applications which is in line with the Council's Digital Strategy
- Developments are delivered by a small number of staff working closely together with the active input of users
- Good engagement between Meritec and Council officers

There are a number of actions the Council could take that would give it greater assurance over the security and resilience of its systems and data, which are hosted remotely on Meritec servers, and to ensure that systems developed on the Meritec ESB platform continue to contribute effectively to the Council's vision as captured in the Digital Strategy.

The Council might also wish to consider whether or not a risk register be created for the on-going Meritec ESB development programme to ensure potential risks and mitigating actions are considered and captured.



Audits reports at draft

We have 6 audit's at draft report stage:

- Economic Development
- CCTV
- ICT Cyber Security
- Newark Cattlemarket
- Creditors
- Assurance

These will be reported to the committee in detail once finalised.

Work in Progress

We also have 7 audits in progress :

- Gilstrap
- Council Offices Gateway review
- HRA Self Financing Business Plan
- Environmental Protection
- NSDC Companies
- Development Company
- Brexit

Details of these can be seen in the 2018/19 plan at appendix 4.

Audits planned for quarter 3 include:

- Emergency Planning
- IT Infrastructure
- Payroll
- Commercialisation
- Key Controls
- Combined Assurance
- Street Cleansing
- Counter Fraud
- Follow-ups

Other Work Completed

We have completed the first review of implemented actions . From the audit work undertaken, we were pleased to report that all six recommendations reviewed have been implemented and relevant business units have retained sufficient evidence which support the actions taken.

Benchmarking

Internal Audit's performance is measured against a range of indicators. The statistics below show our performance on key indicators year to date.

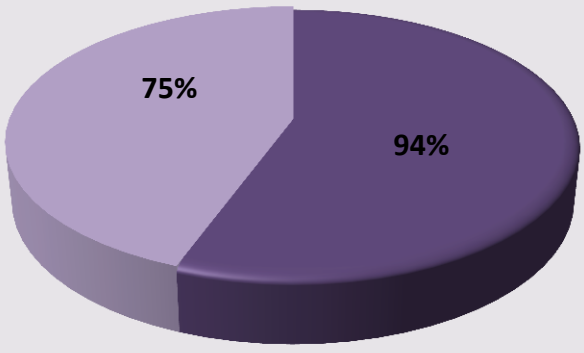
Performance on Key Indicators

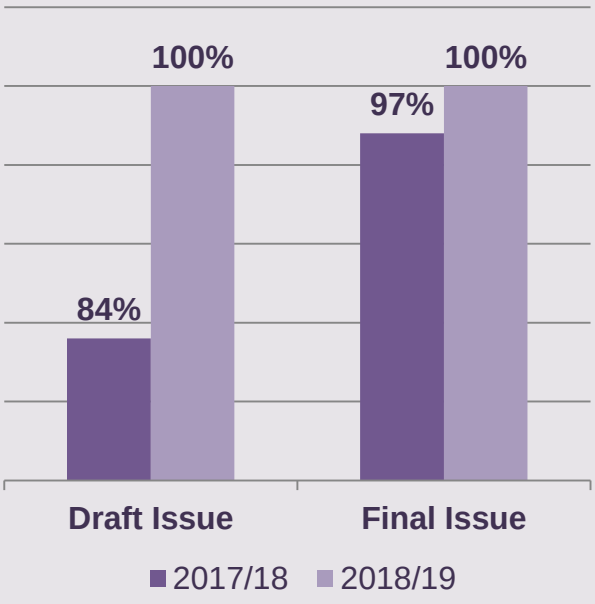
100%

Rated our service Good to Excellent

%

Span – Draft report within 2 months





Appendix 1 Assurance Definitions

High	Our critical review or assessment on the activity gives us a high level of confidence on service delivery arrangements, management of risks, and the operation of controls and / or performance. The risk of the activity not achieving its objectives or outcomes is low. Controls have been evaluated as adequate, appropriate and are operating effectively.
Substantial	Our critical review or assessment on the activity gives us a substantial level of confidence (assurance) on service delivery arrangements, management of risks, and operation of controls and / or performance. There are some improvements needed in the application of controls to manage risks. However, the controls have been evaluated as adequate, appropriate and operating sufficiently so that the risk of the activity not achieving its objectives is medium to low.
Limited	Our critical review or assessment on the activity gives us a The controls to manage the key risks were found not always to be operating or are inadequate. Therefore, the controls evaluated are unlikely to give a reasonable level of confidence (assurance) that the risks are being managed effectively. It is unlikely that the activity will achieve its objectives.
Low	Our critical review or assessment on the activity identified significant concerns on service delivery arrangements, management of risks, and operation of controls and / or performance. There are either gaps in the control framework managing the key risks or the controls have been evaluated as not adequate, appropriate or are not being effectively operated. Therefore the risk of the activity not achieving its objectives is high.

PCIDSS

Limited Assurance

Current Rating (R-A-G)	Recommendations (All High Priority)
Risk 1 - Management arrangements for progressing PCI DSS compliance are not effective.	
Recommendations Implemented	0
Recommendations Outstanding	1
Risk 2 - Failure to comply with PCI DSS	
Recommendations Implemented	0
Recommendations Outstanding	2

Background and Context

PCI DSS is the Payment Card Industry Data Security Standard. This is a worldwide standard that was set up to help businesses process card payments securely and reduce card fraud. It does this through tight controls surrounding the storage, transmission and processing of cardholder data that businesses handle. PCI DSS is intended to protect sensitive cardholder data.

PCI DSS is a recognised standard comparable to other information security frameworks such as ISO:27001. Compliance with the PCI DSS standard will help ensure that payment card data is secure and adopting the standard more widely throughout the organisation will help ensure the Council has increased resilience against threats to all of its data.
If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- fines for the loss of this data
- fraud losses incurred against the cards involved
- banks operational costs associated with replacing the accounts.

Scope

An earlier audit report on PCI DSS compliance, issued in May 2016, gave a limited assurance opinion. This review has focused on evaluating the progress made on the recommendations within that report and the assurance level that can now be given.

The Council should annually self-validate its PCI DSS compliance. Should a card data breach occur then the bank may investigate and determine whether the Council's assessment of its compliance was accurate. In undertaking our assessment we have therefore adopted a strict interpretation of the guidance provided by the Payment Card Industry Security Standards Council.

Executive Summary

We found that the Council has not progressed the required documentation and evidence to support the annual PCI DSS compliance assessment. As a result the Council is not PCI DSS compliant and we can only give a limited assurance opinion at this time.

We are aware that additional pressures have been experienced in that the Council relocated its premises, which diverted a lot of IT resources, notably those of the Assistant IT Manager who led on PCI DSS compliance. Shortly thereafter the Assistant IT Manager then left the Council.

Executive Summary - Continued

This position has not been filled, although PCI DSS compliance has now been picked up by a member of staff within the IT section.

The Council may have access, through its acquiring bank (the term acquiring bank denotes the independent financial institutions which authorise and process credit card payments on behalf of merchants), to an online portal that could help with the PCI DSS compliance process. We have raised this matter with both the IT and Finance teams and have made a recommendation to determine whether this online portal is available to the Council as this would likely greatly simplify compliance work.

Our recommendations from the previous audit review, undertaken in May 2016, are largely restated with requirements to:-

- Confirming the availability of an online portal with the acquiring bank to assist PCI DSS compliance. If this is not available, then annual formal project arrangements are put in place to ensure a staged approach to compliance is undertaken.

- Annually identify and document all of the system components within the Council that interact with cardholder data. Determining this scope is foundational to complying with PCI DSS. Without a clear understanding of scope, the Council cannot validate its boundaries and would not know where to apply the requirements.

- Complete the relevant self-assessment questionnaire (SAQ). The SAQ is designed as a self-validation tool to assess security for cardholder data. The Self-Assessment Questionnaire includes a series of yes-or-no questions. If an answer is "no", the Council may be required to state the future remediation date and associated actions to resolve to a "yes".

The Council is however aware of the need under PCI DSS to undertake quarterly scans of its network, and we have confirmed that a scan has been undertaken in the past quarter.

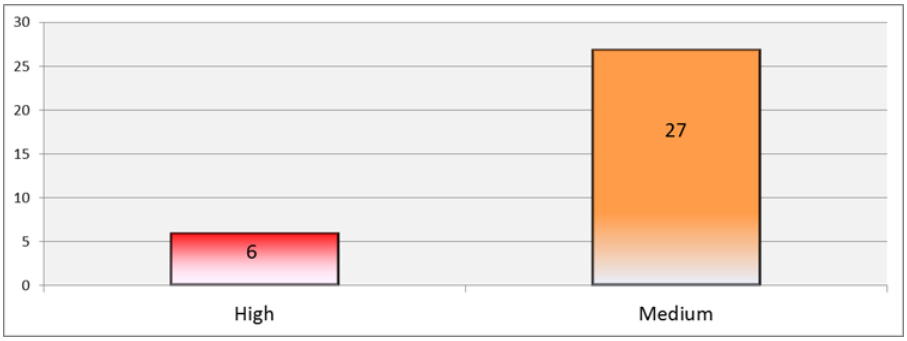
Management Response

ICT accept the recommendations included within the report and will give appropriate focus and commitment to addressing the issues to complete the compliance.

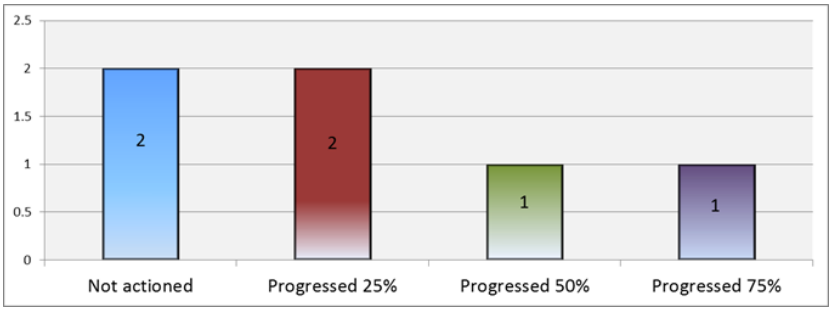
Appendix 3 Details of Overdue Actions

Outstanding Audit Actions for all audits at 30 September 2018

All Actions remaining to be implemented



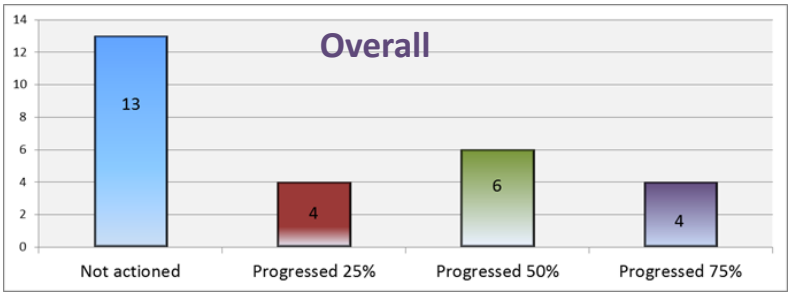
High Priority Actions remaining to be implemented



Overdue Recommendation

Audit	Finding Recommendation	Action Description	Action Current Due Date	Action Owner
Health and Safety	4.1 The training arrangements are reviewed ensuring all staff are given an opportunity to attend Health and Safety and general risk management training 4.2 Refresher training is regularly provided ensuring all staff are kept up-to-date with Health and Safety requirements and reminded of their responsibility. 4.3 Management ensure Health and Safety training modules are developed for staff and consider whether completion of any course needs enforcing i.e. making them mandatory	As part of any H&S training offer devised we will consider whether courses need to be made mandatory.	30/09/18	Ben Adams

Medium Priority Actions remaining to be implemented



Appendix 4 2018/19 Audit Plan to date

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
Mansfield Crematorium	Completion of the audit of the Mansfield Crematorium Accounts	Apr-18	Apr-18	May-18	Completed
HRA Self Financing Business Plan	There is a business plan in place which is up-to-date, based on sound assumptions and reported.	May-18	May-18		Fieldwork
S106 Funding	There are effective processes in place for the receipt and spending of S106 monies.	May-18	May-18	Aug-18	Substantial
Emergency Planning	Arrangements are in place which enable the Council to effectively manage an emergency planning situation.	Jun-18			Awaiting completion of other audit before starting.
Economic Development	The Council has an economic development strategy in place which sets out it's objectives and actions. The projects/schemes/processes used to achieve the objectives are robust and authorised.	Jun-18	Jun-18		Draft Report with client
Cyber Security	The Council has arrangements in place to safeguard it from a cyber security attack. If it does suffer an attack there are effective processes to contain it and reduce it's affect on the Council's business.	Jun-18	Jun-18		Draft Report
Newark Cattlemarket	Completion of the rent calculation for 2017/18	Jun-18	Jul-18		Drafted
Creditors	There are effective processes and procedures in place which ensure that payments are made to the correct suppliers in a timely manner and in accordance with the Council's Financial Procedure Rules.	Jul-18	Aug-18		Draft Report
Development Company	There is an action plan in place for the establishment of the Company and governance arrangements which follow best practice. The establishment of the Company is authorised.	Jul-18	Jul-18		Fieldwork
Assurance	The responsibilities of the assurance function are clearly defined and embedded enabling the provision of accurate and up-to-date reporting of compliance and monitoring of corrective measures.	Aug-18	Aug-18		Draft report with CMT
Brexit Preparation and understanding the risks and opportunities	The Council is aware of the potential implications of Brexit and keeps abreast of these as the process progresses. These implications are identified within any strategic planning for the Council and it's wholly owned companies.	Aug-18	Sep-18		Fieldwork
Gilstrap	Independent Examination of the Gilstrap accounts in accordance with S145 of the Charities Act 2011.	Aug-18	Sep-18		Completed all but one query
NSDC Companies	Review of the Governance and processes in place for the Council's wholly owned companies.	Sep-18	Sep-18		TOR
Review of IR35	There are processes in place which ensure that the Council identifies all those affected by IR35 and payments are made in the correct manner.	Sep-18	Aug-18	Oct-18	Substantial
Environmental Protection	Licenses are issued where statutorily required with income being collected and accounted for. Inspections are carried out and documented in accordance with legislation.	Sep-18	Oct-18		TOR
IT Infrastructure	Review of various aspects of the Council's IT infrastructure which may include security of IT assets; network security; physical security; firewall security; remote access portals / virtual private networks; operating system reviews; web security; internet and email security; anti-virus and malware; penetration testing;public services network; and incident management.	Oct-18			

Appendix 4 2018/19 Audit Plan to date - continued

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
Payroll	The processes and procedures in place ensure that only authorised payments are made to staff and members in a timely manner.	Oct-18			
Commercialisation	There is a clear strategy and action plan in place covering the Council's commercial aspirations and this conforms with the relevant legislation.	Oct-18			
Key Control Testing	Delivery of key control testing to enable Head of Internal Audit to form an opinion on the Council's financial control environment.	Nov-18			
Combined Assurance	Updating the assurance map and completing the Combined Assurance report.	Nov-18			Meetings arranged
Street Cleansing	An efficient and effective service is in place which ensures that streets are maintained at the level of cleanliness expected.	Dec-18			
Counter Fraud	Strategies and policies are in place for the prevention and detection of fraud.	Dec-18			
Domestic Refuse	The service provided is efficient and effective with any income due to the Council being collected and accounted for. Action is taken to resolve customer complaints which are monitored and used to improve performance.	Jan-19			
Strategic Asset Management	There is an up-to-date Strategic Asset Management plan in place and reported. All Council assets are recorded and maintained by the Council or in accordance with any agreement.	Jan-19			
Project/Programme Management	There are effective arrangements in place which ensure that all projects are recorded, allocated responsible officers/teams and overseen allowing an overarching view of capacity and identifying any benefits or efficiencies.	Jan-19			
Workforce changes and succession planning within the Council including changes within the management team	The Council has a workforce plan in place which meets the changing needs of the Council and the demographic and skills of staff. There is also a plan in place for succession planning of key staff identifying positions which hold the greatest risk if vacant i.e. specialist knowledge, statutory responsibility, lone workers etc.	Jan-19			
Business Continuity	Follow-up review to assess the progress being made on the implementation of the recommendations made and ownership has been assigned.	Feb-19			
IT Governance	The Governance arrangements of the IT service ensure that there are processes in place and roles and responsibilities are clearly identified.	Feb-19			
Running of elections and Referendums	There are arrangements and policies in place which ensure that the Council effectively manages the election and referendum processes and payments in accordance with the electoral commission guidelines.	N/A	N/A	N/A	Cancelled
Follow-ups	Follow-up of recommendations made for the progress report and on a sample basis.	Mar-19			1 completed