GA.59 16/17	
Governance & Audit Committee	
17 January 2017	

C

Subject: Internal Audit Quarter 4 Progress Report 2016/17

Report by:	Lucy Pledge (Head of Service – Corporate Audit & Risk Management – Lincolnshire County Council)
Contact Officer:	Ian Knowles, Director of Resources Ian.knowles@west-lindsey.gov.uk
Purpose / Summary:	The report gives members an update of progress, by the Audit partner, against the 2016/17 annual programmes agreed by the Audit Committee in March 2016.

RECOMMENDATION(S):	1) **Members consider the content of the report and identify any actions required.**

IMPLICATIONS

Legal: None directly arising from the report

Financial: FIN REF 9/18

Staffing: None.

Equality and Diversity including Human Rights:

NB: A full impact assessment **HAS TO BE** attached if the report relates to any new or revised policy or revision to service delivery/introduction of new services.

None arising from this report

Risk Assessment: N/A

Climate Related Risks and Opportunities: None arising from this report

Background Papers: No background papers within Section 100D of the Local Government Act 1972 were used in the preparation of this report**.**

Call in and Urgency:

Is the decision one to which Rule 14 of the Scrutiny Procedure Rules apply?

Yes		**No**	**X**

Key Decision:

Yes		**No**	**X**

West Lindsey District Council
The Entrepreneurial Council

Assurance LINCOLNSHIRE

For all your assurance needs

Internal Audit Progress Report at 31ST March 2017

Contents	Para

Appendices to Accompany Report

Contact Details:
Lucy Pledge CMIIA QIAL
Head of Audit & Risk Management

Assurance LINCOLNSHIRE

For all your assurance needs
County Offices, Newland, Lincoln, LN1 1YG
☐: **01522 553692** ☐**lucy.pledge@lincolnshire.gov.uk**

Introduction

1. The purpose of this report is to:

   - Advise of progress made with the 2016/17 Audit Plan
   - Provide details of the audit work undertaken since the last progress report.
   - Provide details of the current position with agreed management actions in respect of previously issued reports
   - Raise any other matters that may be relevant to the West Lindsey Governance & Audit Committee role

Key Messages

2. Work continues to progress on the revised 2016/17 audit plan with all audit reviews either started or at draft report stage. Four audits have been completed since the last progress report and five are currently work in progress. Details are included in the Internal Audit Plan schedule in Appendix 2

3. The annual assurance mapping process is complete and the Combined Assurance report and Annual Audit plan for 2017/18 have been presented and approved by the G&A committee.

4. We have delivered 84% of the 2016/17 Internal Audit Plan. Appendix 2 provides details on the current status of the plan.

5. Good progress has been made in implementing audit recommendations - there is currently only one overdue action. This is the 2012/13 ICT Infrastructure Review which was Limited Assurance. The overdue action is High priority. Details on the outstanding actions can be found in Appendices 3 and 5.

6. Work in progress includes – Progress & Delivery review – draft report with GCLT. Intelligent client review, draft report planned for April 2017, ICT Application review (The Flare system), draft report planned for April 2017, key finance control testing, draft report planned May 2017 and Programme and Project management, draft report planned for April 2017.

Internal Audit work completed at 31ST March 2017

7. The following audit work has been completed and final reports have been issued since the progress report presented to the January meeting of the audit committee:

High Assurance	Substantial Assurance	Limited Assurance	Low Assurance	Consultancy
None	ICT Incident Management Follow up review. Risk Management Growth	ICT PCI DSS	None	None

Note: The Audit Committee should note that the assurance expressed is at the time of issue of the report but before the full implementation of the agreed management action plan. Definitions levels are shown in Appendix 4.

8. Below are summaries of the audit reports issued. :

ICT Incident Management follow up review – Substantial Assurance

In July 2016 we completed a review of Incident Management to provide assurance that ICT incidents are promptly identified, recorded and investigated in accordance with the Councils agreed incident management process. We also reviewed that sufficient and appropriate actions are taken to ensure the ongoing security of the Councils infrastructure and data.

The review gave a low assurance opinion on the controls examined and as a result management requested that a follow-up review be undertaken to confirm that remedial measures had been implemented.

The original review proposed 7 recommendations which were scheduled to be implemented by the 31st August 2016.

We carried out a follow up review in December 2016 and found that Incident Management arrangements are much improved since the original review took place, with the bulk of the recommendations being implemented and work being undertaken to progress those that are outstanding. The arrangements in place now provide a "substantial" level of assurance.

Risk Management – Substantial Assurance

A key indicator for good governance and assurance on the Councils delivery of corporate aims, service delivery and project management is having effective risk management systems in place.

For our review we considered the following areas –

- Review and test the risk management systems in place for strategic risk management.
- Verify the service level risk management processes is robust and communicated.
- Ensure staff understand the risk management approach and engage in risk management and monitoring across all services.

We found there are effective risk management processes in place for managing strategic and service risks. There are clear codes of practice in place which although need a slight update still clearly lay out the Councils expectations for the management of risk.

Strategic and service risks are centrally recorded, regularly reviewed, discussed and reported to management groups and the process is firmly established and understood. Managers showed a good awareness and understanding of monitoring, managing and considering risks as part of everyday service operations.

With firm foundations in place to manage and monitor risks the Council could now look to strengthen its processes by moving the focus of current monitoring from ensuring risks are up to date to include the quality and accuracy of the recorded risks.

There is an opportunity to review how project and partnership risks are recorded and monitored. This is a more fluid area than strategic and service risks with potentially greater risks and rewards to be managed. The Council has detailed large scale plans for both Commercial and Growth projects to support corporate aims and at the time of the audit the recording and monitoring of some project and partnership risks was not as well established as the strategic and service risk management.

Growth – Substantial Assurance

This audit sought to give independent assurance on the effectiveness of the current governance arrangements and project management processes to support the delivery of the ongoing growth programme.

Based on the work completed for the early stages of the programme development, the current governance arrangements and the project management processes in place are operating adequately ensuring successful progress on the growth programme delivery. Our assurance is based on the early development work completed.

We found several areas where the governance arrangements, processes and controls are working effectively including:-

- Dedicated Projects and Growth Team is established which is responsible for the day to day operations of the Growth Programme and associated projects.

- The Growth Programme priorities are aligned to the Council's Economic Growth Strategy and the Corporate Plan objectives
- Specialist consultants e.g. lawyers, architects and other companies are consulted for advice, support and guidance on technical matters related to the programme
- The Growth Board reviews and agrees the Growth Programme and projects before recommending to the relevant committees for approval.
- Strategic sites are identified and acquired to support the current and future commercial development needs.
- Regular progress reports (including highlight reports) are produced for the Growth Board
- To ensure continuity, the Strategic Lead, Economic Development and Neighbourhoods is appointed to the post of Commercial Director.

Some areas were identified where improvements are required to strengthen the processes and governance arrangements supporting the programme including:-

- Ensuring project management processes are streamlined where necessary and applied proportionately taking into account the complexity and size of the project activity. This will speed up the decision making process and enable staff to focus their time on major projects.
- Incorporating the programme and project risks into the Council's operational risk register and ensuring ownership and responsibility for managing the project risks is defined and understood.
- Provision of project management training to staff supplementing the informal on the job mentoring and the one to one supervisions.
- Monitoring the availability of financial resources required to fund the identified growth programme projects.

Overdue Audit Recommendations

9. Outstanding Internal Audit recommendations are tracked and monitored along with the Council's Business Improvement Officers to ensure actions are accurately recorded and monitored. This helps to maintain oversight and momentum.

10. There is one overdue management action which is High priority, this was originally due 31.12.2013. The latest revised date on record is the 31.07.2016.

    Appendix 3 provides details of all outstanding recommendations.

Performance Information

11. Our performance is measured against a range of indicators. We are pleased to report a good level of achievement against our targets – The table below shows our performance on key indicators as at 31st March 2017.

12. We have worked closely with CGLT throughout the year on amendments and changes to the audits in the annual plan. This has had some effect on the delivery of audits and our actual performance against target to date.

Performance Details 2016/17 Planned Work

Performance Indicator	Annual Target	Target to date	Actual
Percentage of plan completed.	100% (revised plan)	100%	84%
Percentage of key financial systems completed.	100%	0%	*0%
Percentage of recommendations agreed.	100%	100%	100%
Percentage of recommendations due, implemented.	100% or escalated	100% or escalated	100% or escalated
Timescales:			
Draft report issued within 10 working days of completing audit.	100%	100%	100% 6 of 6
Final report issued within 5 working days of CLT agreement.	100%	100%	100% 6 of 6
Period taken to complete audit –within 2 months from fieldwork commencing to the issue of the draft report.	80%	80%	81% 5 of 6
Client Feedback on Audit (average)	Good to excellent	Good to excellent	Excellent 5 of 5

*NB Work scheduled in and due to start April, this will give us the full previous 12 months to review financial transactions.

Appendix 1 – Details of Limited Assurance Reports

ICT- PCI DSS – Limited Assurance

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.

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.

Customers may also opt for alternate, more resource intensive and payment methods. The number of card payments between April 2016 and November 2016 amounted to 21,153 transactions.

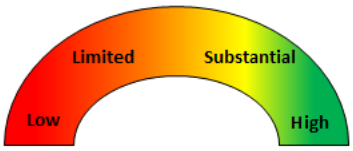
The review will focus on providing assurance that the Council has appropriate arrangements in place to ensure that:

- annual compliance work is undertaken and documented
- any remedial work identified by quarterly network scans is promptly resolved.

Scope

Our audit will include a review of:

- Management arrangements and responsibilities.
- The arrangements in place to ensure compliance with PCI DSS across Council Services where card holder data is required.



Limited Assurance

Risk	Current Rating (R-A-G)	Recommendations	
		High	Medium
Risk 1	Management arrangements for progressing PCI DSS compliance are not effective.	0	1
Risk 2	Failure to comply with PCI DSS	4	3

Key Messages

The Council is not wholly compliant with the Payment Card Industry Data Security Standard (PCI DSS) and as such could be liable to fines and the cost of any resulting fraud losses should a data breach involving card data occur.

Key areas of non-compliance are:

Key Messages

1 Establishing which areas of the Council need reporting on for PCI DSS compliance

The first step of PCI DSS compliance is to accurately determine the scope for compliance, identifying where card data enters the Council. Scoping must occur at least annually. At present the complete card payment environment for the Council is not clearly identified and documented on an annual basis. We found that some payment channels had not been included in the compliance assessment and as such the Council should not be considered compliant at this time.

2 Completion of a self-assessment questionnaire

The second stage is to then complete a self-assessment questionnaire (SAQ). The "SAQ" is a validation tool for merchants (i.e. the Council) to report the results of their PCI DSS self-assessment to their bank. The SAQ includes a series of yes-or-no questions for each applicable PCI DSS requirement. If an answer is no, then the Council may be required to state the future remediation date and associated actions. There are different SAQs available to meet different card-holder data environments.

Because the Council hasn't fully established it's card payment environment we are of the opinion that the current SAQ type being used isn't right. This could mean that the Council isn't responding to the right questions relevant to its card data environment and could be deemed by the bank to be non-compliant with the PCI DSS standard should a breach occur. As a result the Council could be assessed by the bank to be non-compliant.

We examined the SAQ that the Council had completed and found several responses to be inaccurate. The responses given could lead the bank to believe the Council is compliant when in reality this may not be the case.

In terms of assessing the risk we have considered that the Council is not wholly compliant with PCI DSS standards. There is always a chance for a data breach to occur but there are other controls in place that go towards mitigating this.

The impact of a data breach occurring is however significant and could give rise to costs being incurred, e.g.:

- Fines associated with non-compliance following a data compromise; these can range from ten to hundreds of thousands of pounds.
- Liability for the costs of fraudulent activity if the Council is found to be non-compliant.
- Covering the cost of a PCI Forensic Investigator if deemed necessary. The cost of a forensic investigation can run into thousands of pounds.
- The Council's ability to take card payments could be revoked.
- Reputational damage that could deter the use of card payments by service users.

- In addition to the fines imposed by the bank the UKs Information Commissioner also has the power to levy fines associated with data breaches up to a value of £500,000.

The Council's bank can also impose a monthly non-compliance charge if the responses provided by the Council in their PCI DSS submissions confirms them to be non-compliant.

Areas of Good Practice

Staff responsible for taking payments are required to sign an undertaking confirming they are aware of the need to safeguard card data and to report any suspected breaches.
The payment processing function for card payments is undertaken by a chosen supplier whose application is PA DSS (Payment Application Data Security Standard) compliant, thereby reducing the risks to the Council associated with certain PCI DSS requirements.

The Council's bank also provides an online portal that guides and simplifies the compliance process.

Management Response

Although the overall level of assurance provided by the audit is limited, the work undertaken has identified a number of improvements that can be quickly made in order improve matters. One reason for the issues identified is that responsibility for co-ordinating the PCI submission was held by an officer who has subsequently left the Council and hand over of responsibility to a colleague was not fully effective in setting out the purpose of the PCI submission and the protocols and processes to follow. Hence it has been a case of 'learning on the job' which has resulted in an inaccurate evaluation of the scope for compliance (i.e where card data enters the Council) and the subsequent inaccurate completion of the SAQ. Steps have been made to remedy this position by ensuring all involved in the subject matter are involved in PCI submission work to ensure the accuracy of scope and the provision of accurate responses to the SAQ.
The issues which could be regarded as complying with best practise are recognised and will be implemented.
The security of data is a key priority of the Council and the remedial actions will strengthen our position and form part of our overall staff awareness procedures and training. We would like to request a follow-up audit after nine months to ensure that matters have been addressed.
We would like to thank the auditor for the rigour with which they have conducted this audit and their willingness to discuss and explain in more detail their findings.

Appendix 2 – Audit Plan Schedule

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
Development Management Services Consultancy Phase 1	Phase 1 c/fwd from 15/16, consultancy to provide advice and support on the management of improvement plans to support the long term development of the service.	Q1	Not started		Cancelled
Development Management Services Consultancy Phase 2	Phase 2, provide assurance that improvement plans and changes have led to better outcomes and a sustainable Development Management Service.	Q4	Not started		Postponed to 2017/18
Commercial Plan Phase 1	Phase 1 consultancy to provide advice and support on the governance and management structures in place to support the Council's Commercial Plan objectives.	Q1	June 2016	September 2016	Complete
Commercial Plan Phase 2	Provide assurance on the management and delivery of the key Commercial Plan themes. Review how services and key projects are structured and align to the commercial plan deliverables and objectives.	Q4	Moved to 2017/18		WIP
Key Policies and Procedures	Up to date policies and procedures play a key part in management assurance. We will confirm that key	Q1	June 2016	September 2016	Complete Substantial

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
	policies are up to date, understood and followed.				
Progress and Delivery	Provide assurance on the P&D reporting process. Reviewing accuracy and relevance of key performance measures used in reporting.	Q3	September 2016		Draft report with GCLT
Risk Management	Review strategic and Service level risk management to give assurance on the effectiveness of monitoring and management of risks.	Q3	September 2016	March 2017	Complete Substantial
Growth Programme	Review and provide assurance on the governance and effectiveness of the Council's growth plans and agenda.	Q3	December 2016	March 2017	Complete Substantial
Service Transformation	Provide assurance that new delivery models are fit for purpose and align to the medium term financial plan and corporate objectives.	Q2	Not started		Cancelled replaced by EB audit in 2017/18
Intelligent Client Partnership Review	Using contingency days provide assurance on how the Council manages key partnerships and ensure WLDC officers can take a leading role partnership development.	Q3	Feb 2017		WIP
ICT Audit 10 days – Flare	Area of coverage to be agreed	Q4	March 2017		WIP

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
ICT PCI DSS – Security of Electronic payment records	To review the Council's compliance with PCI DSS systems.	Q3	November 2016	Feb 2017	Complete Limited
Consultancy and Emerging risks.	Audit time available for work not identified in the annual plan.	Q1 – Q4			Cancelled
Project & Programme Management	Review the changes to the Councils governance arrangements and project management arrangements. Including the realignment of boards and management responsibilities.	Q3	December 2016		WIP
Key Control Testing	Delivery of key control testing to enable the Head of Internal Auditor to form an opinion on the Council's financial control environment.	Q4	April 2017		Ready to start
Contingency Days – ICT Incident Management Follow Up	Follow up the Q1 low assurance audit to confirm that findings have been implemented.	Q4	December 2016	Feb 2017	Complete Substantial
Housing Benefits Subsidy	Test a sample of benefit cases to on behalf of the external auditor KPMG to provide assurance on the subsidy claimed by the Council	June 2016	June 2016	October 2017	Complete - Consultancy no opinion
Combined Assurance Mapping		Oct 2016	Oct 2016	March 2017	Complete Combined Assurance report

Appendix 3 - Overdue Audit Recommendations at 31st March 2017

Data is for audits where recommendations were due to be implemented by 31ST March 2017

Activity	Issue Date	Assurance	Total Recs	Recs implemented	Priority of Recommendations o/s		
					High	Medium	Not yet due
ICT Infrastructure	August 2013	Limited	15	14	*1	0	0

* Original date for completion December 2013. Revised date July 2016.

Appendix 4- Assurance Definitions[1]

High Assurance	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 Assurance	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 Assurance	Our critical review or assessment on the activity gives us a limited level of confidence on service delivery arrangements, management of risks, and operation of controls and / or performance. 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 Assurance	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.

[1] These definitions are used as a means of measuring or judging the results and impact of matters identified in the audit. The assurance opinion is based on information and evidence which came to our attention during the audit. Our work cannot provide absolute assurance that material errors, loss or fraud do not exist.

Appendix 5- Details on overdue audit recommendations 2016/17

Name	Priority	Finding	Agreed management action	Date to be completed	Response Comments	Revised date for completion	Person responsible
WLDC_ICT_ Infrastructure 12/13	High	A 'high-level' IT strategy is being produced, however we were advised that it may not cover the use of 'shared' resources across authorities, including for example people and IT resources. The draft ICT strategy was not seen during the audit.	Agreed Gareth Kinton (ICT Manager) will progress the recommendation for a detailed IT strategy with the business. It is recognised that the IT strategy should 'align' with other strategies from partner Authorities to whom closer integration may be required in the future.	31/07/2016	The ICT strategy has been in development for some time and whilst a full strategy has not been agreed during that period the development and progression of the Corporate ICT has continued to be developed. An ICT Strategic Overview was agreed with Corporate Policy and Resources in June 2015 and in recent months we have had SOCITM undertaking work to review our current plans and carry out maturity surveys of IT and Digital provision. Whilst an IT strategy is still intended to be delivered this will now be aligned with the work on our Closer to the Customer (CTTC) programme which is currently being scoped.	31/07/2016	James O'Shaughnessy

End of report