West Lindsey District Council
The Entrepreneurial Council

Assurance LINCOLNSHIRE
For all your assurance needs

Internal Audit Progress Report at 30th June 2018

Contents **Para**

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 2018/19 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 finalising the 2017/18 audit plan and we have started work on the 2018/19 annual plan.

3. The following audits have been completed since the last progress report and details are included in this report:

   - Procurement
   - PCI DSS Follow Up
   - ARCUS Consultancy
   - The Portfolio Board

   2018/19 quarter one audits currently in progress are

   - The Growth Programme
   - Environmental Protection

   Quarter two audit preparation includes agreeing Terms of Reference (TOR) for -

   - Customer First Programme review
   - Financial Strategy and Budget Preparation
   - Budget Monitoring

   Full details of progress are detailed in the Internal Audit Plan schedule in **Appendix 2.**

4. Work continues on the Governance review and this is planned to be completed in quarter three and then reported to Committee. This audit has run across 2017/18 and 2018/19 and is planned to be completed as part of this year's work plan.

5. We have delivered 9% of the 2018/19 Internal Audit Plan against a quarter one target of 18%. We have been completing the final 2017/18 audits and of the three reviews due in quarter one two are underway, with one at draft report stage. The final review due for quarter one is going through management approval to agree the terms of reference.

6. Good progress has been made in implementing audit recommendations - there is currently no overdue action to report. There is one action where we have received an update and a new date for completion has been added. This relates to the section 106 part of the Development Management audit, which was substantial assurance. Details on the outstanding actions can be found in **Appendix 3 & 5**.

Internal Audit work completed at 30th June 2018

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

High Assurance	Substantial Assurance	Limited Assurance	Low Assurance	Consultancy
	Procurement Portfolio Board	PCI DSS Follow Up		ARCUS

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. :

Procurement – Substantial Assurance

Continued funding cuts and service transformation means that it is essential that the Council manages it's spending through a structured approach to procurement, to ensure value for money (VfM) and fairness and transparency in allocating public contracts.

This review sought to provide assurance on the effectiveness of the current guidance and procedures in place to manage effective procurement.

Our review found that the Council's approach to procurement is clearly defined within Contract Procedure Procurement Roles (CPPR's), Financial Procedure Rules and a Code of Practice, and staff

are supported in its application by the Council's Contract and Procurement Officer, and a designated Procurement Lincolnshire contact.
Our review tested seven large scale procurements where the Council had been supported by Procurement Lincolnshire. The sample of contracts tested had been completed in compliance with CPPR's.

We found some areas in the smaller procurements, not supported by procurement Lincolnshire, and some areas in overall corporate procurement processes and policy where controls, records and compliance with CPPR's need to be strengthened.

We agreed an action plan with management to address these.

Payment Card Industry Data Security Standard (PCI DSS) Follow Up – Limited Assurance

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.

An earlier audit report on PCI DSS compliance, issued in March 2017, 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 has provided answers in respect of card data security to the online PCI DSS portal supplied by the Council's bank. The portal has reported that the Council is now compliant but we would advise that this is a result of the Council's use of self-validation tools and this then doesn't verify or test what the Council provides.

Our own assessment is that the Council still has work to do in order to assure itself that it is compliant with the Payment Card Industry Data Security Standard (PCI DSS) and it is our opinion that there is a significant risk that, whilst the Council has assessed itself as compliant, it is not.

A number of recommendations from the original PCI DSS audit report remain outstanding and we have identified two further issues that we would like management to address and respond to.

Further details of this report are attached at Appendix 1.

ARCUS – Consultancy

The Council had commenced a project to implement ARCUS Planning, a cloud based ICT system for Development Management, Building Control and Land Charges. The project was seeking efficiency and productivity gains through more modern software offering that provided visible performance information to officers and managers assisting officers to work remotely and directly to the Councils customers via the internet.

The Council took the decision to terminate the project, due to issues around the delivery of the systems as proposed by the supplier.

Our review identified a number of areas where improved project management could have benefited the overall deliver of the project, including –

- Ensure the project manager coordinates the procurement through the Procurement team from the start of the project, following the Councils Contract Procedure Rules.
- Ensure that project managers fully follow project management duties allowing decisions to be made objectively and with maximum benefit to the project outcome.
- Ensure full evidence is collated to support the supplier answers and where possible supplier clients are visited independently and systems reviewed to ensure the supplier will deliver systems as per tender.
- PM and project board to ensure that communication is maintained with supplier throughout the project lifecycle, with mechanisms for any significant issues to be immediately raised and resolved.
- Project board to review the project risk register throughout the life of the project to ensure emerging risks are being captured and fully documented and addressed as they arise.

There were a number of positive outcomes acknowledged as a result of the project. Each department had the opportunity to review their departmental processes. The Land Charges department was able to reduce their application process time down from an average of 26 days to 8 days year up on year and have now been tracking an average of 4 days for the last 6 months. Both the Planning & Development and Building Control departments have reviewed the contents of their letters and number of letters sent out, and these have been streamlined to make the letters more customer focused.

Portfolio Board – Substantial Assurance

The Portfolio Board's remit is to provide oversight and corporate leadership of all key projects and programmes ensuring there is effective sponsorship, resource allocation, governance and delivery of programme and projects.

The aim of the review was to provide assurance that the Portfolio Board is operating effectively in managing the development and delivery of key programmes and projects of work. We attended board meetings, reviewed supporting documents and spoke to key board members as part of our review.

Our observations and review found there is more clarity and purpose in the way the board runs than we have found in a previous review of the Councils key governance board.

During 2017 we completed a review of the commercial strategy and effectiveness of the Entrepreneurial board and found the board was not providing effective oversight of projects and programme management. We found that the Portfolio Board is working well in carrying out its remit of providing management oversight, support and challenge to the council's larger scale projects and programmes.

The summary reports which go to the board give a detailed snapshot and overview of programme and project management which allows the board to scrutinise and support delivery and progress. Key officers and project managers attend which allows the board to challenge, support and provide a strategic and operational view of the Councils programmes of work, which is fulfilling its remit.

There were four findings included in the report to support more effective governance, review and management oversight, including;

- Ensuring all the required information on finance, risks and milestones are completed
- Reviewing the assurance process which rates each project with an indicator to inform the board if it is on track. To ensure a consistent measurable process is applied.
- Having a focus on high risks identified and missed milestones to provide transparency and records that projects have been scrutinised.
- Ensuring there is clarity on the governance board structure for the Portfolio Board and sub programme boards.

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 management action with a revised date for completion from the section 106 review.

Appendix 3 & 5 provides details of all outstanding recommendations.

Other matters of Interest

Lincolnshire Audit Committee Forum

The Lincolnshire Audit Committee Forum is a networking group which enables the sharing of good practice, emerging governance and risk issues and hot topics for public sector audit committees. It is designed to help and support the effectiveness of audit committees.

This is good opportunity to meet up with members of audit committees countywide and we plan to host an all-day forum event on 16th October 2018. This forum day is open to all members of public sector Audit Committees.

CIPFA Publication – Audit Committees – A Practical Guide for Local Authorities and Police (2018 Edition)

This publication sets out CIPFA's guidance on the function and operation of audit committees and represents good practice for audit committees in local authorities throughout the UK.

It emphasises the importance of audit committees and recognises the key part they play in governance. The publication covers:

- Core functions
- Possible wider functions
- Independence and accountability
- Membership and effectiveness
- Suggested terms of reference
- Audit committee members – knowledge and skills framework

Performance Information

11. Our performance is measured against a range of indicators. The table below shows our performance on key indicators as at 30th June 2018.

Performance Details 2018/19 Planned Work

Performance Indicator	Annual Target	Target to date	Actual
Percentage of plan completed.	100% (revised plan)	18%	11%
Percentage of key financial systems completed.	100%	0%	*0%
Percentage of recommendations agreed.	100%	100%	0%
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%	0% (None Issued)
Final report issued within 5 working days of CLT agreement.	100%	100%	0% (None Issued)
Period taken to complete audit – within 3 months from fieldwork commencing to the issue of the draft report.	80%	80%	0% (None Issued)

Client Feedback on Audit (average)	Good to excellent	Good to excellent	

*Work scheduled in and due to start January / February 2019, this will give us almost a full 12 months of financial transactions for the review.

Appendix 1 – Details of Limited Assurance Audits

PCI DSS Follow Up

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.

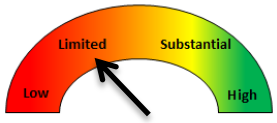
If an organisation loses card data and is not PCI DSS compliant then there is the potential for financial penalties to be imposed such as:

- 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 March 2017, 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 annually self-validates 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.



Risk	Rating (R-A-G)	Recommendations	
		High	Medium
Risk 1 - Management arrangements for progressing PCI DSS compliance are not effective.	Green	**0**	**0**
Risk 2 - Failure to comply with PCI DSS – **Recommendations outstanding**	Amber	**1**	**3**
Risk 2 - Failure to comply with PCI DSS – **New recommendations**	Amber	**1**	**1**

Key Messages

The Council has provided answers in respect of card data security to the online PCI DSS portal supplied by the Council's bank. The portal has reported that the Council is now compliant but we would advise that this is a result of the Council's use of self-validation tools and this then doesn't verify or test what the Council provides.

Our own assessment is that the Council still has work to do in order to assure itself that it is compliant with the Payment Card Industry Data Security Standard (PCI DSS) and it is our opinion that there is a significant risk that, whilst the Council has assessed itself as compliant, it is not.

A number of recommendations from the original PCI DSS audit report remain outstanding and we have identified two further issues that we would like management to address and respond to.

We would further suggest that the Council acquaints itself with the current (v3.2) Data Security Standard as this will provide further insight into the questions posed by the bank, and the rationale behind them.

Additionally, there is a template document for "Reporting on Compliance" used by independent assessors to confirm PCI DSS compliance, which may also assist in the Councils completion of its PCI DSS tasks.

Key Messages

Recommendations we found not to have been implemented are listed below:

- Annual Scoping Exercise – High Priority

The first step of PCI DSS compliance is to accurately determine the scope for compliance, identifying where card data enters the Council. Scoping must

documented. This has not been undertaken in the past year.

- Completion of a self-assessment questionnaire – High Priority

The second stage is to then complete a self-assessment questionnaire (SAQ). The "SAQ" is a self-validation tool for merchants (i.e. the Council) to report the results of their PCI DSS self-assessment to their bank.

Our earlier review found that some of the responses within the complete SAQ were incorrect. However, there are different questionnaires available to meet different environments. The Council has since progressed an earlier audit recommendation to identify the correct SAQ to be completed, but our assessment remains that some of the responses to one of the current SAQs is not supportable and should be reviewed.

Inaccurate responses could lead the bank to believe the Council is compliant when in reality this may not be the case.

- Completion of Network Diagrams – Medium Priority

Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise. Current network diagrams were not provided as part of this review. The requirement to do this is linked to the responses in the self-assessment questionnaire to which the Council has said is not applicable. We believe this may not be correct.

- Inspections – Medium Priority

Payment devices should be periodically inspected to make sure they haven't been tampered with. There isn't a proper inventory of payment devices (as required under 9.9.1. of the PCI standard) and neither is there any documentation to evidence the periodic checking of these devices.

Areas of Good Practice

The Council has progressed the following recommendations:

- Upwards Reporting Of Compliance Progress – Medium Priority

A recommendation to report to management progress on PCI DSS compliance has been adhered to in that we are informed that the Director of Resources (and Senior Information Risk Owner) was informed that

compliance was achieved in respect of payment terminals at the Council and payments taken by staff over the phone. The response to the original recommendation was that confirmation of compliance would be reported to the Corporate Information Governance Group but this has not taken place and staff involved with PCI DSS compliance have questioned whether this is the right group to monitor compliance.

- Determination of correct Self-Assessment Questionnaire to complete – High Priority

In order to determine which type of self-assessment questionnaire the Council needs to complete, it responds to an initial set of questions set by the bank. In our assessment, the responses to these initial questions are accurate and we therefore have confidence that the correct Self-Assessment Questionnaires are being completed.

- Development of a PCI DSS Security Policy and Training for staff – High Priority

The Council has produced a very informative security policy for staff that handle credit and debit cards. A training module has also been established and rolled out, although management need to ensure that the completion rate for this training is improved.

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. The portal also identifies any in-year tasks that need to be recorded, such as the annual review of the Information Security Policy.

The Council's PCI DSS Security Policy is clear and informative, providing good direction for the control of card holder data and payment devices used within the Council. The Council has also implemented an e-learning module on card data security for staff that are responsible for taking card payments.

As a standard process, the Council undertakes background checks on all new starters. Whilst this is a requirement under PCI DSS, it is something that the Council was already doing under its own initiative.

Management Response

While the findings of this audit have not produced the result we would have wanted, it does demonstrate that progress has been made since the last audit. We have developed a PCI DSS Security Policy, sourced and rolled-out training for staff, introduced a schedule for checking our payment devices, adopted a collective effort around the process and put in place arrangements to report to the Council's SIRO. While a number of issues remain to be worked through, we continue to work to achieve greater assurance in our processes and security concerning the receipt of card payments. This is a highly technical subject, for which differing interpretations are possible and this is one reason for the auditor finding that our compliance status may not be as secure as we previously thought. Steps will be made to address this and we will make greater use of the guidance that is available to support us in this. Other matters to address relate to the systematic recording of actions/decisions and the completion of training by relevant colleagues.

It is important to stress that as far as we are aware, customers have had no issues or had their security compromised when making card payments; with this method of payment being greatly utilised as residents signed up and paid for the Council's Green Waste service. Additionally the bank has not reported any issues with our arrangements.

As is our policy when receiving a limited assurance finding we would like to request a further follow-up audit in Q3 of this year to further assess and test our procedures.

We would like to thank the auditor for his work, his preparedness to be challenged on the findings and the expert advice he has provided.

Appendix 2 – Audit Plan Schedule

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
Environmental Protection & Enforcement	Review the recent changes in structures and management and provide assurance that services are being delivered as intended.	**Q1** June 2018	June 2018		WIP
Income and Investment programmes	Review the Councils approach to managing projected gaps in the budget and provide assurance on the delivery of projects which provide a commercial return to the Council.	**Q1** June 2018			To agree TOR
Growth Programmes from 17/18	To follow up on 2016 growth audit work and provide assurance on project and programme work in delivery.	**Q1** May 2018	June 2018		WIP
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	**Q2** Dependent on external auditor.			Not started
Customer First	A key programme of work and business transformation for the Council. Provide assurance that the programme is being effectively managed and monitored.	**Q2** July – Sept 2018			TOR Agreed
Corporate Planning	Review the Council's systems and processes over the setting of its strategic direction.	**Q2** July – Sept 2018			Not started
Financial Strategy &	Review the Councils systems and processes in	**Q2** July – Sept			TOR agreed

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
Budget Preparation	place to provide assurance on the management of budgets. This will include budget setting, forecasting, monitoring, any key person dependencies and system access.	2018			
Budget management	Review the Councils systems and processes in place to provide assurance on the management of budgets. This will include budget setting, forecasting, monitoring, any key person dependencies and system access.	**Q2** July – Sept 2018			TOR agreed
Leisure Contract	Consultancy review of the new Leisure contract process.	**Q2** July – Sept 2018			
ICT Areas to be agreed		**Q3** Oct – Dec 2018			
Follow up PCI DSS	Follow up low or limited audit reports for assurance on improvement and implementation of findings	**Q3** Oct – Dec 2018			
Follow up Sales & Invoicing	Follow up low or limited audit reports for assurance on improvement and implementation of findings	**Q3** Oct – Dec 2018			
Combined Assurance	Document the Councils critical areas to provide an assurance rating to	**Q3** Oct – Dec 2018			

Area	Indicative Scope	Planned Start Date	Actual Start Date	Final Report Issued	Current Status / Assurance Opinion
	inform the audit plan and report to management and members.				
Follow up Planning Enforcement	Follow up low or limited audit reports for assurance on improvement and implementation of findings	**Q3** Oct – Dec 2018			
Follow up Commercial	Follow up low or limited audit reports for assurance on improvement and implementation of findings	**Q3** Oct – Dec 2018			
10 Unallocated contingency days	To be used to address any arising areas of risk or control identified in year.	**Q4** Jan – Mar 2018			
Key Controls Finance	Delivery of key control testing to enable the Head of Internal Audit to form an opinion on the Council's Financial control environment.	**Q4** Jan – Mar 2018			To start Jan – Mar 19

Appendix 3 - Overdue Audit Recommendations at 30th June 2018

Data is for audits where recommendations were due to be implemented by 30th June 2018

Activity	Issue Date	Assurance	Total Recs	Recs implemented	Priority of Recommendations o/s		
					High	Medium	Not yet due
Development Management	October 2017	Substantial	9	8	0	1*	0
Totals			**9**	**8**	**0**	**1**	**0**

*Original date for completion 31.03.2018, revised date 01.10.2018.

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 2018/19

Name	No.	Priority	Finding	Ref	Status	Agreed management action	Date to be completed	Response Comments	Revised date for completion	Person responsible	Rating
WLDC 2017/18-Q1 - 02 - Development Management		Medium	There is no current regular reporting of section 106 information. It is planned that when the new ICT system ARCUS goes live this will be addressed. However at the time of the audit the ARCUS project had stalled and was behind schedule. Implementation was due in April 2017 but the provider was not able to keep to agreed deadlines for delivery and in August 2017 the system was not implemented. . This would be particularly valuable not only to management but also to residents and members. As section 106 agreements represent the public getting something back when a new development is agreed in their area.	05.1 - s106 reporting	Not Implemented	Review work objectives and agree a robust system of reporting as an interim measure until the ARCUS system is implemented.	31.03.2018	On track for delivery in October: The first part - to implement a CIL monitoring system is complete and live. This is being extended to capture all s106 and associated trigger points for payments. CIL had to be prioritised after Members formally agreed to adopt CIL early in 2018. The s106 element is almost entirely complete for the system development, data capture is now ongoing to populate the database. Note - there is no P&D requirement to monitor s106 information, however the new system would allow this if Members were to require updates. Already, the work to improve the data held has entirely eliminated historic issues with s106 records that were identified in the audit. Press articles to promote where s106 monies have been collected (eg Market Rasen Skate Park) have been used to improve understanding and awareness of how s106 is collected and used.	01.10.2018	Oliver Fytche - Taylor	Substantial

End of report