Lincolnshire COUNTY COUNCIL
Working for a better future

Regulatory and Other Committee

Open Report on behalf of Judith Hetherington Smith, Chief Information and Commissioning Officer

Report to:	**Audit Committee**
Date:	**22 June 2015**
Subject:	**Information Governance Breaches – Internal Audit**

Summary:

This report is to provide an update to the position reported at the Audit Committee meeting on 30th March 2015.

Following a number of information breaches involving Lincolnshire County Council information an internal audit was requested by the Chief Information and Commissioning Officer. The aim of the audit was to provide management assurance on a number of key information governance areas including; training and awareness; security incident reporting; and third party information sharing and processing.

The audit resulted in a number of recommendations aimed at improving current information governance practices across the Council. This report describes activity undertaken so far to meet these recommendations.

Recommendation(s):

The Committee is asked to note the progress being made against the recommendations described in this report.

1 Background

Information Governance is a key function which requires a multi-disciplined approach across every aspect of the Council involved in handling, processing and sharing information.

It supports the relevant legal and compliance requirements the Council must abide by and assists in maintaining public confidence in the way the Council delivers services and improves the effectiveness of business activity.

The information governance structure and approach adopted by the Council has been subject to much positive change over the past 12 months and continues to develop in its maturity. The findings of the internal audit support ongoing efforts to improve current practices and acts as evidence of a frank and transparent approach adopted by the Council to identify and resolve issues. The internal audit report has also helped to

inform a wider information assurance strategy which has been designed to improve information governance practices on a wider scale.

2 Information Governance Breaches Audit

The results of this audit were reported to the Audit Committee in March 2015; a synopsis of key findings and subsequent corrective action is provided below.

	Key Finding	Action	June 2015 position
1.	There is a lack of effective monitoring of employees completing mandatory annual online Information Governance training across the Council and as a consequence completion levels are low.	A more accurate reporting mechanism, utilising the Agresso ERP application, to identify levels of compliance across mandatory information governance e-learning will be introduced. It will better support the management and monitoring of individuals who fail to undertake the training.	**Incomplete**. Delays encountered due to Agresso and Lincs2Learn applications requiring the synchronisation of staff records which is key to ensuring accurate reporting. Work continues to ensure an acceptable solution is implemented. It is currently anticipated that this should be available by September.
2.	Management need to reinforce the need for staff to undertake information governance training and to be supported with an accurate reporting mechanism.	Once accurate reporting is in place, as described above, reports are to be made available to managers to help support monitoring of employee training. A communication plan will be implemented which will promote the importance of training.	**Incomplete.** Delays encountered due to Agresso and Lincs2Learn applications requiring the synchronisation of staff records which is key to ensuring accurate reporting. Work continues to ensure an acceptable solution is implemented.
3.	Refresher training should be provided which is less time consuming and focuses on key issues	A revised e-learning training package will be developed which reduces completion times and focuses on issues relevant to the Council.	**Partially complete.** Creation of a revised training package is underway. Target completion time for staff undertaking training has been reduced from 3 hours to 45 minutes. The reduction in the

			completion time for the revised training has removed the need for an abbreviated refresher training package. Deployment of the training will be achieved in conjunction with the new reporting method as described in Key Point 1.
4.	Accurate records of individuals completing information governance training via an alternative method to the online E learning are not kept.	The information governance team will record training provided by them via other methods e.g. face to face	**Complete**. Instances of alternative training sessions are now being recorded by the information governance team.
5.	Information Governance training does not give prominence to reporting security incidents or measures that should be adopted when sharing information with 3rd parties.	Adapt the training to include more information on the importance of security incident reporting and information processing by 3rd parties	**Complete**. The revised training, which is due to be deployed, now includes more information on reporting security incidents and sharing information with 3rd parties.
6.	Third parties processing information on behalf of the Council must be identified to ensure appropriate safeguards are in place across information processing.	The actions agreed by the Information Security and Compliance Manager differ from those recommended by the audit report to take into account the need for change on a wider scale. Introduce an information asset register designed to identify key information assets (those involving personal and/or sensitive data); Introduce and apply the concept of Information Asset Owners across Director Areas to support appropriate	 **Partially complete**. A business case is currently being drafted to present to CMB. It is currently anticipated that this will be submitted in July **Partially complete**. A business case is currently being drafted to present to CMB.

		management of information. Introduce at the beginning of any information sharing process a consistent approach to information governance requirements. Introduce a privacy impact assessment process, based on Information Commissioners Office best practice. to help identify privacy risks at an early stage of projects involving the sharing of information, The introduction of an information sharing register managed by the information governance team. This will provide a more thorough oversight of sharing where IG assistance has been requested.	It is currently anticipated that this will be submitted in July **Partially complete.** A suite of information governance terms and conditions for contracts which will be used as a reference point are currently being produced by colleagues in Legal. It is currently anticipated that these will be available by August An information sharing agreement template has been produced to standardise and simplify the documenting of such agreements. **Complete.** **Complete.**
7.	A review of security incident management procedures should take into account Information Commissioners Office (ICO) and Health and Social Care Information	A new internal procedure document will be created to formalise and standardise the internal approach and will consider both ICO and HSCIC guidance.	**Complete.**

	Centre's (HSCIC) guidance.		
8.	The method of recording security incidents is basic, relying on the use of an excel spreadsheet. An alternative more complex recording solution will add benefit to the overall process.	An alternative solution to recording breaches and investigation correspondence will be investigated with a view to replacing the basic functionality provided by Excel.	**Ongoing.** A request to utilise Lagan, a web-based CRM solution already utilised by the Council, has been made. This will support wider information governance requirements and will be reviewed to understand its potential benefit as a tool to record security incidents.
9.	Following a security incident containment action, and its appropriateness, is not always documented.	A new internal procedure document will be created to formalise and standardise the internal team approach. This will include the requirement to document and communicate containment measures.	**Complete**.
10.	There is no formal process which considers the severity of an incident with external reporting requirements.	An impact matrix will be developed to assist in achieving consistent internal and external reporting	**Complete**.
11.	Evidence of Caldicott Guardians being notified of security incidents is rarely recorded.	A new internal procedure document will be created to formalise and standardise the internal team approach. This will include the requirement to document where Caldicott Guardians have been advised about specific incidents. Note: The Information Security and Compliance Manager has challenged this finding as it did not consider the context of incidents. E.g. Caldicott Guardians are only advised of data breaches which involve	**Complete.**

		Social Care or Patient data and therefore will not be made aware of every data breach.	
12.	There is no final report issued following an investigation into a security incident breach and as a consequence there is no natural closure of the incident	A security incident final report will be introduced to formally capture recommendations made to staff following a breach and to provide closure.	**Complete**.
13.	Remedial actions that have been agreed following a security incident are not followed up to confirm their implementation.	Follow up of recommendations will be introduced to encourage and improve staff behaviour; to resolve policy gaps; and to improve information processes.	**Complete**.

3 Conclusion

The vast majority of findings articulated within the internal audit report had already been identified by the Information Governance team as processes requiring improvement and as a result corrective action had commenced prior to the internal audit. While good progress continues to be made it is recognised that work is still required on a wider scale to improve the overall information governance framework which will support and encourage organisational buy in and improve good practice.

Coupled with this however is the need for senior managers, managers and staff across the Council to acknowledge the importance of information governance. By adopting appropriate information governance practices and maintaining an awareness of their own responsibilities the information culture of the organisation should improve and the likelihood of information breaches should decrease.

4 Consultation

Policy Proofing Actions Required

n/a

5 Background Papers

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

This report was written by David Ingham, who can be contacted on 553721 or david.ingham@lincolnshire.gov.uk and Judith Hetherington Smith, who can be contacted on 553603 or Judith.HetheringtonSmith@lincolnshire.gov.uk.