Lincolnshire County Council

Information Assurance

Annual Report
2019/20

Contents

Further information available from:

David Ingham
Head of Information Assurance
01522 553721
David.Ingham@Lincolnshire.gov.uk

Foreword

Information is a critical asset that has significant value; without it the council simply cannot function. Therefore the council, its partners, and members of the public, must have confidence in the way information is created, collected, used and shared.

Information, and the systems used to process it, also attract a diverse set of risks which must be understood and confidently managed, maximising opportunities and mitigating risk where necessary in order to support effective service delivery.

Information assurance (IA) provides a mechanism by which the council aims to achieve this by implementing an effective governance and assurance approach to information throughout it's lifecycle, from creation through to destruction.

IA also ensures that we understand, and align with, the legal and regulatory environment within which we operate by using information in a way which is lawful, fair, and transparent, achieving this in a way which helps, not hinders, the delivery of council services.

This annual report summarises activity undertaken by the Information Assurance Team during 2019/20 and reflects the output of 3 core specialist areas delivered by 10 IA staff.

Executive Summary

The Information Assurance Team has, over the past year, continued with its mission of *"embedding an information assurance culture that ensures the council values information, is accountable for the information it uses, and ensures it uses information responsibly, securely and fairly."*

This is demonstrable across all aspects of IA and is presented through the implementation of new controls, improved management information and upwards reporting, improved engagement with staff, and a focus on continued IA development.

5 Key Assurance Messages

- All identified IA risks that are outside of the current risk appetite are subject to ongoing risk treatment plans. Subject specific risk registers and risk treatment plans allow the right resource to target the right activity. All other identified risks continue to be monitored.

- Strong relationships remain with technical colleagues within the councils IMT function and Serco, to ensure a joint approach to the cyber threat. This has resulted in direct improvements to the councils cyber security posture and cyber security reporting metrics.

- The Records Management project continues to tackle historic issues identifying and indexing over 20,000 service user files across the council estate within the last 8 months. This directly reduces corporate risk.

- Continued improvement to the council's Record of Processing Activity has resulted in more concise and consistent privacy information, and a more detailed, informed view of personal data held by the council. This is has been achieved while reducing the burden on Service Areas.

- The IA team continue to provide substantial support to all areas of the council, with a record level of engagement. This support directly influences effective service delivery through pragmatism and informed decision making.

The fluidity of information processing, the evolving nature of information risk, particularly that evidenced in cyber security, and the need for the council to continue to deliver effective services directly influences the IA approach. While much has been achieved the challenges presented remain perpetual and it is vital therefore that continual development sits at the heart of future IA work.

Data Protection

Summary

Data protection services, which includes the statutory role of Data Protection Officer, have continued to improve and develop. Key to this has been improving visibility of the information we hold and implementing controls which demonstrate that the council understands, and takes responsibility for, the personal data it processes. Working hard to support staff with a pragmatic and realistic approach it has also challenged the myth that data protection prevents staff from delivering effective services.

A number of key challenges remain, not only to strengthen those areas that require improvement, but also to ensure as a council we continue to demonstrate accountability for the personal data we process.

Key Headlines

- Refined the council's approach to information asset management resulting in improved understanding of the personal data we hold and a more logical and efficient process to support information asset owners.

- Developed privacy information across all council functions to increase transparency and help individuals better understand what we do with their personal data and why. This directly supports an individuals rights.

- Created a robust Data Protection Impact Assessment tool to enable the identification of high risk processing – this in turn supports informed risk decision making.

- Proactively engaged with, and developed, partnership working to support and promote the free flow of information.

- Delivered a Data Protection Advisory Service to a number of schools receiving "5 star" reviews for the service provided.

Key Challenges

- Ensuring consistent application of corporate controls across a large organisation delivering diverse services to a large numbers of citizens.

- Establishing a comprehensive view of third parties who process information on behalf of the council and ensuring that the relevant safeguards are in place and are appropriate.

- Achieving a clear understanding of scope and purpose of surveillance camera systems in use across the council and ensuring they meet the required legal and regulatory obligations.

Data Protection – Key Data
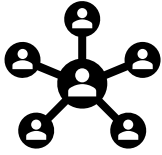
162 projects/tasks requiring extended IA support

25 Information Sharing Agreements created/reviewed to support collaboration

202 council functions reviewed to produce an accurate information asset register.

12 data protection infringements, raised by the ICO, investigated.

7 confirmed data protection infringements

0 enforcement action taken by the ICO

Instances of extended IA support by Directorate

Adult Care and CWB: 38
Children's Services: 44
Commercial: 19
Corporate Services: 4
Resources: 24
Place: 12
Fire, Rescue and Public Protection: 21
Other: 8

Records Management

Summary

There has been significant work undertaken this year to tackle historical issues presented by legacy hard copy records across the council estate. This has already resulted in major improvements, directly reducing corporate risk and improving our understanding of records held. The scale of work required however means this work will continue for some time.

Concurrently, improvements to corporate controls, increased awareness, and improved visibility of the function has improved the value, consistency and simplicity of the approach.

Key Headlines

- Internal audit provides a substantial level of assurance across the Records Management plan.

- New 4 year contract in place with offsite hardcopy records storage provider Restore, ensuring compliance with the General Data Protection Regulation.

- A more efficient mechanism introduced for sending and retrieving hardcopy records from offsite storage.

- Establishment of a 3 year project to address hard copy legacy records held onsite and offsite which has already resulted in significant improvement of preciously unmanaged records.

- Development of corporate retention schedules to better reflect council functions.

- Increase in Service Area engagement at every level of the council directly improving awareness.

Key Challenges

- Continuing to locate, index, and appraise hard copy historic records spread across the council estate.

- Attracting and maintaining Service Area engagement to ensure successful disposal of found records and improving the overall position of records management in the council.

- Increasing awareness of new processes to reduce the likelihood of repeating historical bad practice.

- Understanding the electronic records estate and ensuring resource availability to support future projects.

Hard Copy Records Project

Over 20000
records located and indexed

Including **10000** records relating to Childrens Services

24 key locations holding records identified

Including **10000** records relating to Adult Care

Including **5430** safeguarding records

Including **5980** adult frailty and long term conditions records
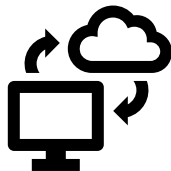
400 staff provided with improved tools to manage record transfers

Over **360** ad hoc requests for records management support

Information Security

Summary

The focus of information security has remained consistent throughout the year centering on the investigation of reported security incidents; undertaking security assurance work of 3rd parties to support service areas manage information risk; and working closely with colleagues in IMT and Serco to improve cyber security controls.
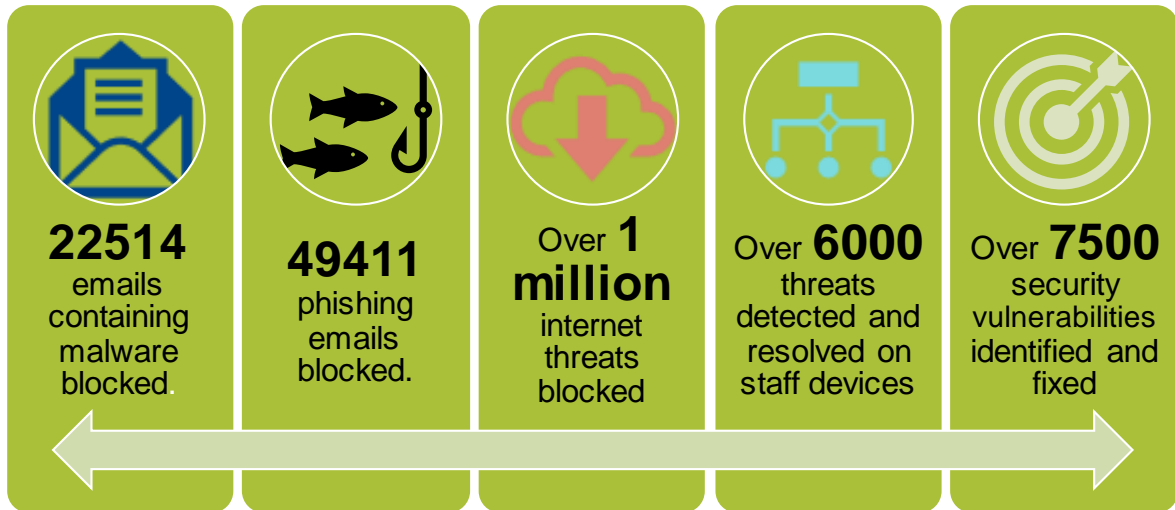
Key Headlines

- Internal audit provides a high level of assurance across IA management of personal data breaches

- Serco, with the support of LCC, achieve recertification against ISO 27001, Information Security Management Systems. The scope includes the council's ICT environment.

- LGA cyber security stock take self-assessment improves from Red/Amber in 2018 to Amber/Green in 2019 with key improvements in organisational controls.

- Working with Serco colleagues a much improved vulnerability management process has resulted in a more robust remediation process of key vulnerabilities i.e. security patching.

- An improved mechanism for encrypting email making it easier for staff to send email securely.

- Increased engagement with the wider security community resulting in improved knowledge sharing and intelligence gathering.

- Positive culture changes which have resulted in a direct increase in the number of security incidents being reported to the IA team. This allows a faster and more efficient response.

Key Challenges

- Ensuring a thorough and consistent approach to assuring cloud services.

- Maintaining organisational awareness of the cyber threat, particularly threats from malicious email e.g. phishing.

- Supporting IMT/Serco colleagues to improve the diverse set of cyber security controls needed to protect council assets.

- Reducing the number of security incidents caused by human error.

- Achieving the right balance between security and usability by ensuring security does not become a blocker.

Information Security – Key Data

Cyber controls

22514 emails containing malware blocked.

49411 phishing emails blocked.

Over **1 million** internet threats blocked

Over **6000** threats detected and resolved on staff devices

Over **7500** security vulnerabilities identified and fixed

Security Incidents Reported to the IA Team

Status	Cause	Data Type	Nature of Incident
317 reported and investigated	**89%** human error	**154** involving personal data	**207** unauthorised disclosure
259 confirmed security incidents	**2%** malicious activity	**72** involving Special Categories of Personal Data	**25** loss of data/hardware
12 data breaches reported to ICO	**2%** policy or process gap	**9** involving other sensitive data	**10** failure to safeguard

11598 highest number of malicious emails blocked in a single month

44 third party security assurance tasks completed

**95%** of security incidents had a negligible impact on the council

Summary

Training and awareness has remained a key activity throughout the year with a particular focus on cyber attacks and records management. There has been comprehensive engagement across all Directorates and at every level to support ongoing knowledge and understanding. The outcome has been a direct increase in IA engagement and visibility, improved security incident reporting, and increased awareness of information risks, particularly those relating to cyber threats.

Maintaining a reasonable level of awareness across the council remains a key objective which must take into account the needs of a diverse set of services.

IG E LEARNING – STAFF COMPLETION

Year	Completion
17/18	85%
18/19	90%
19/20	86%

104 Internal comms circulated
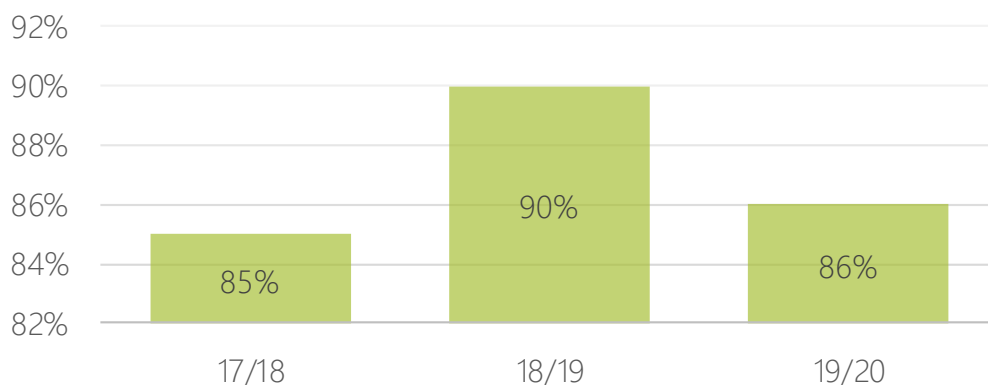
27 cyber security presentations delivered

43 Information Asset Owners directly engaged

30 records management training presentations

Appendix 2 – Key risks

The IA Team manage risk registers concerned with Cyber Security; Data Protection; Record's Management and general IA. The table below reflects 3 key risks.

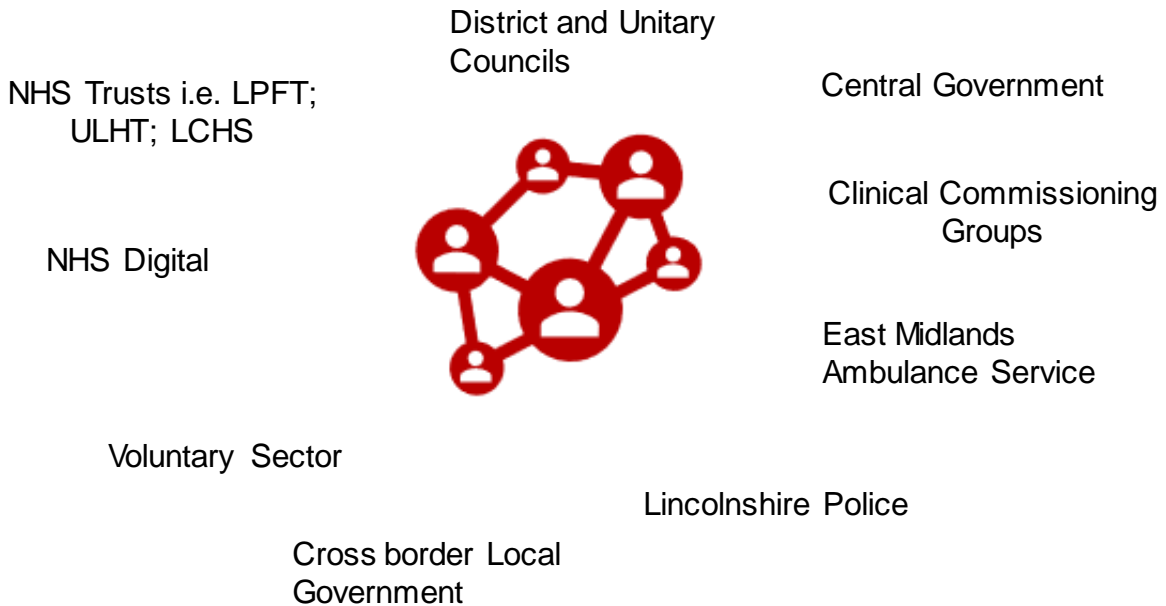| Risk	Raw rating	Current rating	Target rating	Risk travel
There is a risk of a **successful cyber attack** against the council which will have a **significant/critical impact**. (This risk is jointly owned by IMT)	16	12	8	↓
Comment: The evolving nature of cyber threats means this is an ever present risk which requires consistently robust and diverse technical and organisational controls. Currently sound organisational controls are in place which remain under constant review. Improvements to technical controls are ongoing with the focus on two key controls, which when implemented should reduce the risk to the target rating. Managing this risk requires long term effort and investment.				
There is a risk that the councils legal obligations will not be met because of an **inconsistent and fragmented approach to hard copy records management**.	12	12	6	↓
Comment: This risk is largely due to the historic management of hard copy records resulting in dispersed holdings of uncontrolled records across the estate. A project has been initiated and is coming to the end of year 1 of 3. It is making excellent progress resulting in the identification and indexing of thousands of records allowing service areas to make informed decisions about next steps. Alongside project work improvements are being made to every aspect of the corporate approach including improved support, and more efficient processes.				
There is a risk that that the council **is unable to meet it's legal obligations under the Data Protection Act 2018 and General Data Protection Regulation**.	16	12	6	↓
Comment: Significant work has been undertaken to put in place a corporate approach which assists the council in meeting its data protection obligations. The approach focused on areas of key risk. There remains areas which require improvement which are mainly the execution of corporate controls at an operational level and consistency in the corporate approach.				

Key

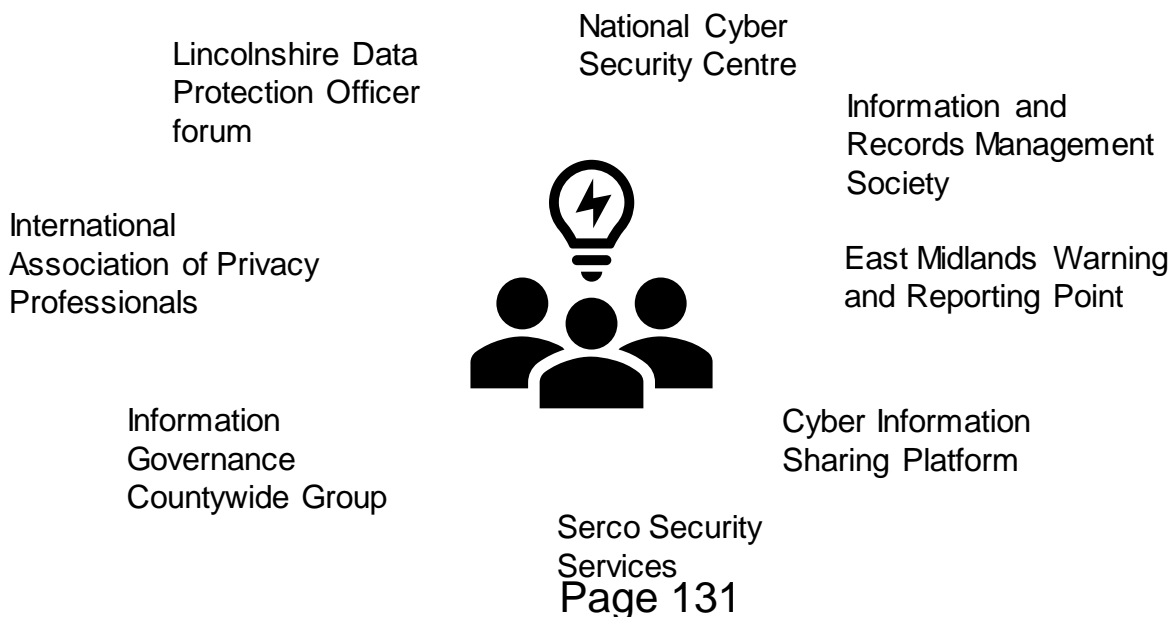| Likelihood				
4 Almost certain	4	8	12	16
3 Probable	3	6	9	12
2 Possible	2	4	6	8
1 Hardly ever	1	2	3	4
Impact	1 Negligible	2 Minor	3 Major	4 Critical

Appendix 3 – External Engagement

IA supports all service areas at every level of the council. In addition we actively engage with a variety of external partners and agencies to support effective partnership working and knowledge sharing. This directly benefits delivery of council services.

Partnership working

District and Unitary Councils

NHS Trusts i.e. LPFT; ULHT; LCHS

Central Government

Clinical Commissioning Groups

NHS Digital

East Midlands Ambulance Service

Voluntary Sector

Lincolnshire Police

Cross border Local Government

Knowledge Sharing

Lincolnshire Data Protection Officer forum

National Cyber Security Centre

Information and Records Management Society

International Association of Privacy Professionals

East Midlands Warning and Reporting Point

Information Governance Countywide Group

Cyber Information Sharing Platform

Serco Security Services

This page is intentionally left blank