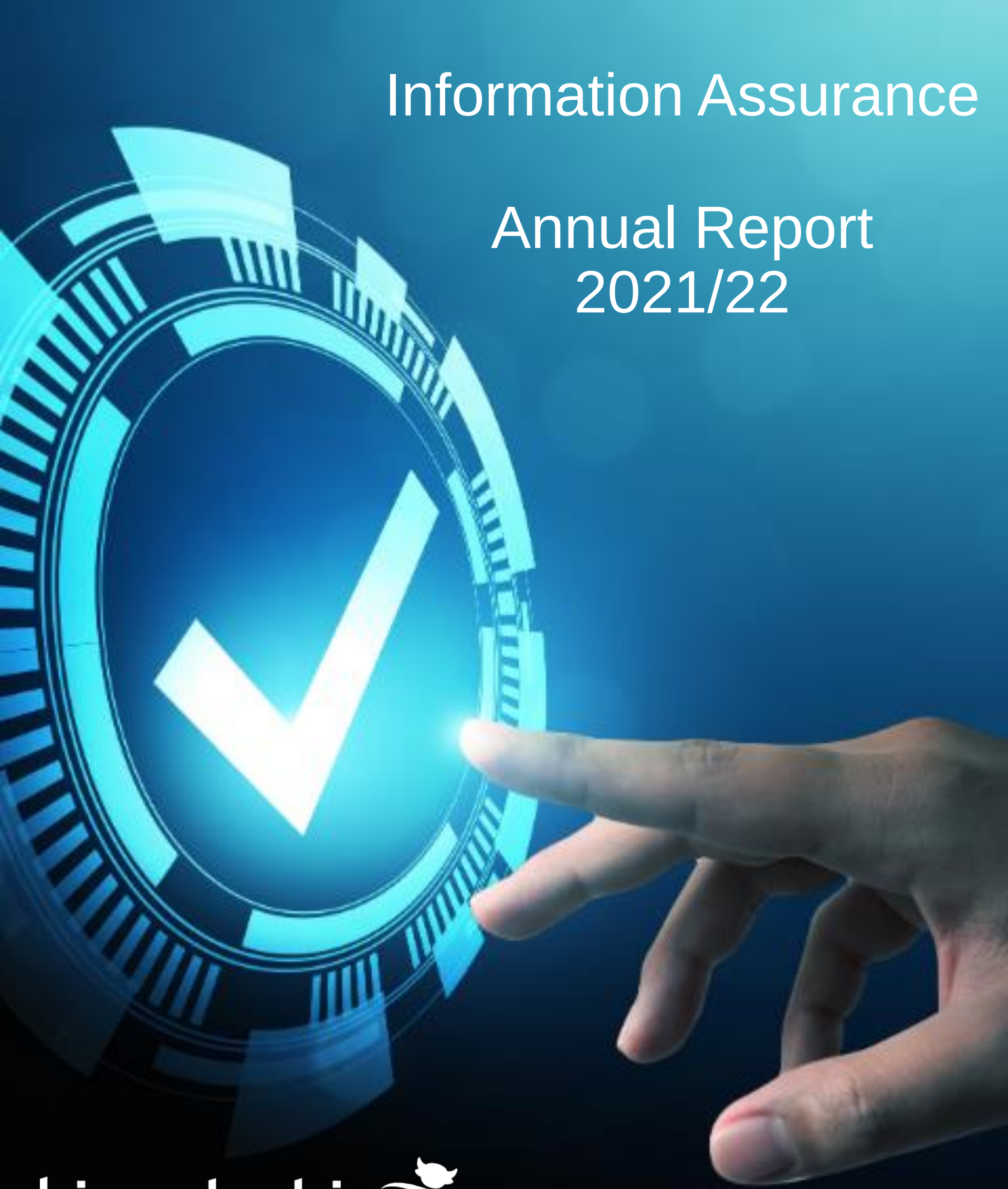
Information Assurance

Annual Report 2021/22



LincoInshire
COUNTY COUNCIL
Working for a better future

Table of Contents

Foreword

Information Assurance (IA) is a cornerstone of any organisation that relies on information to deliver its services and to operate effectively. This is particularly true of local government, which collects and uses diverse and sensitive information created internally and entrusted to us by members of the public and strategic partners.

IA supports effective governance by implementing a corporate framework designed to identify and manage information risk, implement controls which are reasonable and achievable, and encourage informed decision making. IA also helps the council to meet its legal and regulatory obligations, by ensuring that information, particularly personal data, is used in a way that is lawful, fair, transparent, and secure.

Of equal importance is that IA positions itself in a way that supports the council's business plan, by ensuring good value council services and by helping, not hindering, effective service delivery and operation.

This annual report summarises key activity undertaken by the IA team during 2021/22 and reflects the output of three core specialist areas delivered by 11 council officers.

David Ingham
Head of Information Assurance
07876 148551
David.Ingham@lincolnshire.gov.uk

Executive Summary

While the delivery of IA services in 21/22 continued to support the council's response to COVID19, in the latter part of the year there was also a sense of normal service being resumed. Key themes for the reporting year included continual improvement of service delivery, improved awareness and engagement, and promoting the benefits of IA support.

Focusing on these areas resulted in a record high number of requests from colleagues for support. In turn, this presented opportunities to improve controls across various areas of the organisation thereby helping the council to reduce information risk.

The diverse nature of IA support is clear to see from Children's Health Services to Trading Standards; from Special Educational Needs and Disabilities to Independent Mobility Assessments; and from Travel Services to Registered Care Home projects. The IA team has supported colleagues across the council to deliver their services throughout 21/22.

5 Key Assurance Messages

- The single biggest risk to the council remains a successful cyber attack which results in significant or critical negative impact to the council. IA has ensured the organisational response has remained relevant and has continued to support both technical and non-technical colleagues in improving the council's response to this risk.

- Raising and maintaining awareness of IA subject matter remained a key organisational control. Examples included the development of an IA Hub on the Council's intranet offering advice and guidance in plain English (which has already attracted thousands of visits), as well as continual promotion of IA services and support through internal communications and engagement.

- With the lifting of restrictions significant improvements to the overall records management position have been made. Support from CLT has been very positive and a robust plan has been implemented which continued to tackle current and emerging risks across legacy, displaced, and offsite records.

- Formal contact with the Information Commissioner's Office, the UK's independent authority set up to uphold information rights and data privacy for individuals, has fallen due to a reduction in the number of reportable personal data breaches and data protection complaints received.

- IA engagement across every level of the council remained very high not only in the support of individual service areas but also across key corporate projects, including the Business Intelligence Strategy, Microsoft 365 deployment and Smarter Working. This level of engagement demonstrates a positive IA culture

Data Protection

Data protection support not only supported internal services, but it also included multi-agency collaborative working, particularly across health and social care, as well as suppliers and commissioned services. The Data Protection Advice Service for Schools also continued to deliver effectively.

By maintaining high levels of engagement, the IA service has been able to recommend, and help implement, controls designed to reduce privacy risks across diverse areas of data processing.

A focus on presenting advice in a concise and digestible manner, ensuring technical language was translated into plain English, improved accessibility and understanding and has attracted positive feedback. More importantly it has increased the level of support on offer.

Key Headlines

- Five complaints were referred to the Information Commissioners Office (ICO) by members of the public. A single complaint was partially upheld finding that the council had failed to respond to an individual's rights request within the statutory timeframe. A learning point about what constitutes an individual rights request was identified.

- 20 data protection infringements were investigated by the council's Data Protection Officer. Two were confirmed as actual infringements. Learning points about attention to detail in undertaking personal data searches and greater awareness of what constitutes legitimate sharing were identified.

- A new end-to-end process for considering individual rights requests was supported thereby reducing the risk of non-compliance with our legal obligations.

- The service engaged and supported more than 50 individual Information Asset Owners by reviewing the information they hold and ensuring legal obligations continue to be considered.

Key Challenges and Future Focus

- Meeting increased demands and ensuring the right support is provided at the right time with priority given to processing activities which present the greatest risk.

- Ensuring the challenges and opportunities of closer collaboration with strategic partners are understood and planned for.

- Responding to the outcome of the Government's consultation on reforms to the UK's data protection regime.

- Improving visibility across the third parties that process personal data on the council's behalf.

General IA and Data Protection – Key Data

In addition to the hundreds of “simple” support requests, **174** tasks required extended, more complex, IA support:

- **51%** Children’s Services
- **18%** Resources
- **7%** Place
- **5%** Corporate

20% Adults and Community Wellbeing

11% Fire and Rescue

6% Commercial

10% increase in requests for extended IA support.

82% of staff completed IA E learning.

Note: This is based on average employee numbers over a 12 month period.

20 data protection infringements investigated by the council’s Data Protection Officer. A 17% reduction on the previous year.

of these

2 were upheld, with **6** ongoing.

5 data protection complaints reported to the ICO by members of the public. A 50% reduction on the previous year.

of these

1 complaint partially upheld with **2** ongoing.

Records Management

Corporate and service area risk continued to be reduced across holdings of hard copy records as despite a slowing of pace due to COVID19, significantly improved progress was made in the latter part of the year. There is evidence of increased awareness and more productive engagement with information owners. Furthermore, an established and robust appraisal process has identified, reviewed and indexed thousands of records.

Outside of planned work, records management continued to react to requests for support across all formats of records, from both internal services, and external partners and suppliers.

Key Headlines

- The new corporate Records Management Strategy has been published focusing on three key priorities; to understand our records; to improve ownership and awareness; and to review and reduce paper records.

- The corporate records management project has proven to reduce corporate risk by improving overall control and reviewing, indexing, appraising and destroying hard copy records.

- A dedicated onsite records management storage facility was established to enable quicker, more efficient review of displaced and unmanaged records.

- Ongoing records management support continued to encourage better management of digital records through service area and application owner engagement.

- A restructure of offsite records was initiated which will reduce cost and improve knowledge and control of holdings.

Key Challenges and future focus

- Ensuring an efficient response to the requirements of the Smarter Working project, where volumes of displaced records are high.

- Development of record lifecycle workshops to help embed a broader understanding of where records and business value information should be stored and how it can be better managed.

- Supporting application owners to better manage electronic records in new and current systems by improving the record lifecycle.

- Consideration of two ongoing and long-standing legal holds across records which impacts the destruction of records past their retention dates.

Records Management – Key Data

Records Management Project

Over **27000** records identified, appraised and indexed

5000 records destroyed as past retention*

including

18000 client records

6500 HR records

3210 corporate records

Over **1500** boxes of records recovered, packed and moved to support the Smarter Working project

* Two legal holds are in place which has prevented higher number of records being destroyed.

Information Security

Summary

Like all UK organisations, the council continued to deal with a significant volume of cyber attacks. Adding to the challenge were the evolving capabilities and techniques used by attackers. This has required constant effort to reduce the risk of a successful attack. IA ensured the organisational response remained relevant and continued to support technical colleagues in reducing the risks.

An increase in assurance activity driven by service area uptake of Cloud services was also evident. Adopting an approach based on the National Cyber Security Centre cloud security principles directly assisted in reducing risk and improving confidence in the delivery of services.

Security incidents have risen in comparison to the previous year; however, core trends such as root cause and nature of incidents remain constant. Despite the increase, there has been a reduction in the number of data breaches requiring onward reporting to the Information Commissioners Office.

Key Headlines

- A 14% increase in the number of confirmed security incidents investigated by the IA team.
- A 75% reduction in the number of personal data breaches reported to the ICO due to a reduction in breaches involving the most sensitive personal data and improved responses to contain and reduce the impact of reported data breaches.
- A significant increase in the number phishing emails received, up 30% on 20/21 and 60% from 19/20.
- Established improved processes to make it easier to report security incidents and to report spam or malicious email.

Key Challenges and Future Focus

- Keeping pace with the cyber threat and the continual need for an “always on” response.
- Ensuring ongoing organisational awareness of the risks presented by malicious email.
- Providing ongoing support to technical colleagues to improve our cyber security posture.
- Seeking out areas of improvement to reduce the number of security incidents caused by human error.
- Balancing the diverse needs of the council with a pragmatic, but robust, security posture.

Information Security – Key Data

Cyber Attack Prevention

Over 430000 security events blocked on our network perimeter

More than 83000 malicious emails blocked including nearly 80000 phishing emails

Over ½ million internet threats blocked

More than 10000 security fixes applied

Security Incidents

303
total security incidents reported and investigated

263
confirmed security incidents

93%
caused by human error

87%
involving personal data

79%
due to misdirected information

.

Appendix 1 – IA Top Risks

Risk	Raw rating	Current rating	Target rating	Risk status
There is a risk of a **successful cyber attack** against the council which will have a significant or critical negative impact. Note: IA provide the organisational response to support the technical response.	16	12	8	Open and Improving
There is a risk that because of an **inconsistent and fragmented approach to hard copy records management** the council will face action by the Information Commissioners Office or it will lead to large-scale undermining of individual rights	12	9	6	Open and Improving
There is a risk that that the Council is **unable to meet the requirements of the Data Protection Act 2018 and UK GDPR** leading to action by the Information Commissioners Office or large-scale undermining of individual rights	9	6	6	Monitored
There is a risk **that security incidents go unreported or are subject to delay** and as a result the council cannot respond effectively and in a way which minimizes impact and meets data protection reporting obligations.	9	6	6	Monitored
There is a risk that **colleagues lack awareness of their individual information responsibilities and obligations** resulting in an organisational culture that fails to take information assurance seriously.	12	6	6	Monitored

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

This page is intentionally left blank