Assurance LINCOLNSHIRE
For All Your Assurance Needs

West Lindsey District Council
The Entrepreneurial Council

North Kesteven DISTRICT COUNCIL

** DRAFT **

ICT Audit Plan

Date: February 2021

What we do best...

Innovative assurance services

Specialists at internal audit

Comprehensive risk management

Experts in countering fraud

...and what sets us apart

Unrivalled best value to our customers

Existing strong regional public sector partnership

Auditors with the knowledge and expertise to get the job done

Already working extensively with the not-for-profit and third sector

Assurance LINCOLNSHIRE
For All Your Assurance Needs

Contents

The contacts at Assurance Lincolnshire with this report are:

Lucy Pledge - Audit and Risk Manager (Head of Internal Audit)

Lucy.pledge@lincolnshire.gov.uk

Emma Bee - Team Leader

emma.bee@lincolnshire.gov.uk

Stacey Richardson - Principal Auditor WLDC

stacey.richardson@lincolnshire.gov.uk

Amanda Hunt - Principal Auditor NKDC

Amanda.Hunt@lincolnshire.gov.uk

Tony Maycock - Senior Auditor

tony.maycock@lincolnshire.gov.uk

Assurance LINCOLNSHIRE
For All Your Assurance Needs

ICT Audit Planning

Introduction

As part of our 2020/21 combined assurance work, we undertook a detailed review of ICT in order to create a proposed IT Audit plan.

The plans are presented over 3 years to give some indication of future intent. However, our audit plans are flexible and it is likely that risk profiles may change and that new, emerging risks, may present themselves. The ICT Audit Plan will be presented annually.

Developing the ICT Audit Plan

In order to create this plan we focused on mapping assurances against the ISO27001 IT security standard.

Through discussion, we examined each standard to identify what assurances were currently in place. These assurances were then categorised in accordance with the four lines of assurance.

- First Line – Business Management
- Second Line - Corporate Oversight
- Third Line - Internal Audit assurance
- Fourth Line- External Independent assurance

We assessed assurance on over 40 different aspects grouped into the following areas:

- Governance
- Infrastructure
- Operations
- Projects
- Applications
- Compliance Elements (e.g. PSN, PCI-DSS)
- Emerging Risks

ICT Audit Planning

The outcome of our Combined Assurance work was as follows:

High Assurance (Green) – 95%
Medium Assurance (Amber) – 5%
Low Assurance (Red) – 0%

The proposed ICT Audit plans are presented in Appendix A below.

High: Controls in place assessed as adequate/effective and in proportion to the risks.

Medium: Some areas of concern over the adequacy/effectiveness of the controls in place in proportion to the risks'

Low: Significant concerns over the adequacy/effectiveness of the controls in place in proportion to the risks

Annual Evaluation

The assurance map is an evolving document and although it has been used to develop a proposed ICT Audit plan it will be reviewed and updated annually to reflect the current risks and assurances affecting the organisations.

Disclaimer

The matters raised in this report are only those which came to our attention during our internal audit work. Our quality assurance processes ensure that our work is conducted in conformance with the UK Public Sector Internal Audit Standards and that the information contained in this report is as accurate as possible – we do not provide absolute assurance that material errors, fraud or loss do not exist.

This report has been prepared solely for the use of Members and Management of North Kesteven District Council and West Lindsey District Council. Details may be made available to specified external organisations, including external auditors, but otherwise the report should not be used or referred to in whole or in part without prior consent. No responsibility to any third party is accepted as the report has not been prepared, and is not intended for any other purpose. The Head of Audit is only responsible for the due professional care in developing the advice offered to managers on risk, control and governance issues. Where managers accept our advice they accept the accountability for the consequences of implementing the advice. Internal Auditors working in partnership with managers during the consultancy assignment will not take part in any sign off decision.

Appendix A – ICT Audit Plan

2020/21 – Year One

Audit Area	Indicative Scope
ICT Disaster Recovery & Back-Up	Data backup and recovery is the process of backing up your data in the event of a loss and setting up secure systems that allow you to recover your data as a result. Data backup requires the copying and archiving of computer data to make it accessible in case of data corruption or deletion. The review will seek to provide assurance that backups are routinely taken and tested to confirm that a successful recovery can occur and that disaster recovery arrangements are in place and also periodically tested.
Cloud/Housed Services	Review of several cloud hosted solutions to ascertain the level of due diligence undertaken of selected providers, the security arrangements in place and how the arrangements compare to the Cloud Security Principles framework put forward by the National Cyber Security Centre.
Network Infrastructure & Security	Review of the network architecture and design from a security perspective to determine whether adequate security mechanisms are in place and operating effectively. The planned review will encompass the design and configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures that provide guidance on how network security should be managed by both the IT department and users.

Appendix A – ICT Audit Plan

2021/22 – Year Two

Audit Area	Indicative Scope
Network Access Controls: Internal Network Users	Review of arrangements to provide access to new starters, amend permissions for changes in duties and revocation of access for staff leaving the authority. The review will also examine the controls and effectiveness of the application used to automate elements of starters and leavers process.
Network Access Controls: Supplier Access	Review of the governance and technical arrangements to provide supplier access to Council systems.
Network Access Controls: Privileged Account Management	Review to confirm that the allocation and use of privileged access rights is restricted and controlled. Inappropriate use of system administration privileges (any feature or facility of an information system that enables the user to override system or application controls) is a major contributory factor to failures or breaches of systems.

Appendix A – ICT Audit Plan

2022/23 – Year Three

Audit Area	Indicative Scope
Cyber Security	The National Cyber Security Centre (NCSC) has identified 10 steps for cyber security to help organisations manage cyber risks. The review will cover these 10 steps, albeit at a high level, with a view to confirming that appropriate consideration has been given to these areas. Cyber Security and data security has been one of the Institute of Internal Auditors (IIA) top three priority risks identified in their Risk in Focus publications over the past five years. It is documented as the number one priority risk for 2021, and this trend is expected to continue for the next three years.
Patch Management	The review will focus on the patching of software used by Council, and the firmware used in its infrastructure, is kept up to date and safe against known exploits.