



Appendix G ICT Audit Planning

Date: January 2022

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

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

Jill Thomas

Principal Auditor

jill.thomas@lincolnshire.gov.uk

Tony Maycock

Senior Auditor

tony.maycock@lincolnshire.gov.uk

Introduction

Page

1

Production of the ICT Audit Plan

1

Annual Evaluation

2

Distribution List

3

Appendix A – ICT Audit Plan

4



Introduction

As part of our combined assurance work, we undertook a detailed review of the various elements of the ICT service to create the proposed ICT Audit plan.

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

Production of the ICT Audit Plan

In order to create this plan, we focused on mapping assurances against the ISO:27001 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 areas grouped into the following areas:

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

The outcome of our Combined Assurance work was as follows:

- High** Assurance (Green) – 97%
- Medium** Assurance (Amber) – 3%
- 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 organisation.

Distribution List



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.

2022/23 – Year One

Audit Area	Indicative Scope	Days
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.	15
Asset Management: Hardware	To achieve value for money, and full use from the hardware in use it is important that all ICT hardware assets are tracked and managed appropriately. This is increasingly important where staff and equipment are no longer stationary and working from home has become a necessity in response to Covid-19.	15

2023/24 – Year Two

Audit Area	Indicative Scope	Days
Cyber Security	<p>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.</p> <p>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</p>	25

Appendix A – ICT Audit Plan

	number one priority risk for 2021, and this trend is expected to continue for the next three years.	
Virus Protection/Malware	<p>Getting infected with malware - often ransomware - is one of the most common ways that IT systems can be compromised.</p> <p>Malware infection can result in theft of intellectual property, ransoming of data, and/or disruption to services provided by your organisation. As such, it's important for organisations try and prevent malware from being deployed within the Councils network.</p> <p>The audit will provide an objective independent opinion on the adequacy and effectiveness of the control environment with regards to Antivirus and Malware.</p>	10

2024/25 – Year Three

Audit Area	Indicative Scope	Days
Network Access Controls: Starters Movers and Leavers	<p>Review of arrangements to provide access to new starters, amend permissions for changes in duties and revocation of access for staff leaving the authority.</p> <p>The review will also examine the controls and effectiveness of the application used to automate elements of starters and leavers process.</p>	<p>15</p>
Network Access Controls: Supplier Access	<p>Review of the governance and technical arrangements to provide supplier access to Council systems.</p>	<p>5</p>
Network Access Controls: Privileged Account Management	<p>Review to confirm that the allocation and use of privileged access rights is restricted and controlled.</p> <p>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.</p>	<p>15</p>