



Draft ICT Audit Plan (2021/22 – 2023/24)

Date: March 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

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

McJoy Nkhoma

Acting Principal Auditor

mcjoy.nkhoma@lincolnshire.gov.uk

Tony Maycock

Senior Auditor

tony.maycock@lincolnshire.gov.uk

Introduction

Production of the ICT Audit Plan

Annual Evaluation

Distribution List

Appendix A – ICT Audit Plan

Page

1

1

2

3

4



Introduction

As part of our 2020/21 combined assurance work, we undertook a detailed review of ICT in order to create a 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 refreshed and presented annually.

Production of the ICT Audit Plan

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

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 categories:-

- 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) – 62%
- Medium** Assurance (Amber) – 30%
- Low** Assurance (Red) – 8%

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 ICT Audit plan will be reviewed and updated annually to reflect the current risks and assurances affecting the organisation. This will feed into the work undertaken on Combined Assurance.

Distribution List



Director of Resources and Deputy Chief Executive

Business Manager, ICT

Business Manager, Financial Services

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 Newark and Sherwood 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.

2021/22 – Year One

Audit Area	Indicative Scope
<p>Selima HR/Payroll</p>	<p>To provide assurance that the computer security controls within the Selima HR and Payroll system provide a safe and secure operating environment.</p> <p>The current Selima contract expires in November 2022 and the supplier will not be providing any further updates except only system maintenance service. The Council is seeking an alternative system to replace Selima and currently preparing tender documents for the replacement system. The new system will be hosted internally.</p> <p>The 2020-21 Assurance Mapping work indicated a 'High' risk profile for this application. The system uses insecure Hypertext Transfer Protocol (Http) rather than https, which encrypts and decrypts user page requests to ensure secure communication and transaction. The other issue is that password changes for this application system are confirmed by email in plain text which increases the risk.</p>
<p>Cloud Hosted Services</p>	<p>The risks associated with Cloud are wide ranging and varied, and when auditing Cloud or considering the risks you are effectively assessing the whole range of IT risks because whole sections of IT operations are being outsourced to a third party. Often, in the race to migrate to the Cloud, insufficient consideration is given to the entirety of what is required to move to this new operating model.</p> <p>We propose to review recent instances of cloud/hosted services to establish the due diligence undertaken in arriving at the selected option and security deployed through that arrangement.</p>

2022/23 – Year Two

Audit Area	Indicative Scope
<p>Help Desk</p>	<p>The audit will provide assurance that ICT issues reported by users, and service requests, are captured, prioritised and resolved within expected timeframes.</p> <p>The effective management and support of IT assets is a key expectation placed on the shared ICT service. The ICT Help Desks form part of a fundamental and key element of good business service and operation.</p> <p>Through the Help Desk, problems are reported, managed and then appropriately resolved in a timely manner. In doing so, Help Desks can help the Council's service areas run smoothly and improve the quality of the support it offers to the users.</p>
<p>Network Access Controls: Privileged Account Management</p>	<p>The audit will seek to confirm that the allocation and use of privileged access rights to the network are restricted and controlled to ensure the integrity of the systems.</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>

2023/24 – Year Three

Audit Area	Indicative Scope
<p>Cyber Security</p>	<p>The National Cyber Security Centre (NCSC) has identified 10 steps for cyber security to help organisations manage cyber risks. The review will focus on the Council's arrangement to consider and the extent to which the 10 steps have been integrated in the processes to ensure effective management of the cyber-risks and any further guidance is taken on board.</p> <p>Cyber 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.</p> <p>A follow-up review of Cyber-security is taking place in 2020/21 to ensure that previous recommendations and agreed actions have been implemented.</p>