*BARROW BOROUGH COUNCIL*

# INTERNAL AUDIT PROGRESS REPORT

## April to July 2021

## 2021/22

# CONTENTS

**Page**

# EXECUTIVE SUMMARY

## Purpose

The purpose of the report is to update Members of the Council's Audit Committee on:

- Internal Audit work performed up to 16th July 2021, including final reports issued relating to a previous reporting period; and
- Significant issues that have arisen during this period as a result of our work.

## Content

The information is presented in the following schedules:

*1. A Statistical Summary of Recommendations*

This schedule includes all audit recommendations to which Council management have responded between 1st April and 16th July 2021. The figures are analysed according to the 'priority' of the recommendations, and the extent to which each has been accepted by management for action.

*2. Accepted Priority 1 Recommendations*

This schedule provides details of all major recommendations which have been accepted by management.

*3. Rejected Recommendations*

This schedule provides details of major and significant (i.e. Priority 1 and Priority 2) recommendations, which have been rejected by Council Management.

*4. Audit Coverage*

Details of audit assignments carried out in the period, including any checks on external partner organisations.

*5. Classifications of Assurance and Recommendations*

An explanation of the classifications used for prioritising recommendations and assessing levels of assurance.

# 1. STATISTICAL SUMMARY OF RECOMMENDATIONS

The following table summarises the number of audit recommendations we have made in our final reports issued up to 16th July 2021; analysed by their priority, including whether accepted by management.

| Recommendations | Total | Priority 1 | Priority 2 | Priority 3 |
|---|---|---|---|---|
| Made | **7** | 2 | 5 | 0 |
| Fully Accepted | **7** | 2 | 5 | 0 |
| Partly Accepted | **0** | - | - | - |
| Not Accepted | **0** | - | - | - |

# 2. ACCEPTED PRIORITY 1 RECOMMENDATIONS

There have been two Priority One recommendations since the previous Audit Committee, which relate to the following:

| | |
|---|---|
| **Audit Report** | IT75 IT Procedures Review |
| **Recommendation** | The Council should accelerate the completion of the development of a coherent and managed suite of policies that form part of an overarching Information Security Management System. |
| **Rationale** | As part of this review, 13 IT policies along with 284 procedural documents, covering 42 different areas managed or supported by IT were provided. All policies were reviewed along with a cross section of procedural documentation in order to ascertain if the control framework in place was fit for purpose.<br><br>Although there was the basic structure of an Information Security Management System (ISMS) in place, all of the supporting policies/standards had not yet been created to give the required substance for users to be able to comprehensively follow.<br><br>Consulting the Council's IT Strategic Plan 2017-2020, there were some areas that had not been included within the ISMS that should have been, such as risk management, asset management and software copyright and intellectual property rights. It is possible that they may be included within the documents which were not provided for review or those still to be developed, as advised within Appendix A of the Information Security Policy, however, there were no indicative dates for completion provided.<br><br>Without an agreed, current, fit for purpose and suitably communicated complete suite of Information Security Management System policies and procedures, good practice cannot be assured, inconsistencies and non-adherence are more likely and compliance is more difficult to enforce. It is also more likely that a monetary penalty may be issued against the Council in the event of a breach, if it is deemed by the Information Commissioner, that the Council had no specific policies, procedures or processes in place which may have prevented the contravention. The Council engaged a third party to provide a suite of IT policy templates which would form the Council's ISMS structure. Resource was allocated to complete these policies but is no longer available. We have undertaken an internal review of ISMS structure provided by the third party, this is a comprehensive suite of policies and some of them are superfluous to the needs of the Council. We will rationalise the suite so that it fits the needs of the Council. We will identify resource options to update our policies but in the meantime our historical policies are still valid. |

| | |
|---|---|
| **Response** | These templates were marginally different to those previously used. Risk management forms part of the Information management and Security Policy which has not yet been completed and now needs to consider additional controls relating to agile working. Asset Management and software copyright and intellectual property rights are not included in the suite of policies and this will be addressed separately.<br><br>The ISMS policy and end user acceptable usage policies together with new policies covering information assets, and mobile device policies are in place and provide suitable controls to minimise data breaches |

| | |
|---|---|
| **Audit Report** | IT75 IT Procedures Review |
| **Recommendation** | The Council should ensure that all policies undergo the appropriate approval process to ensure it is fit for purpose and is regularly reviewed. |
| **Rationale** | The Council are in the process of fully implementing an Information Security Management System. As part of the audit, thirteen Policies provided by IT were reviewed in order to ascertain if the control framework in place was fit for purpose. The following issues were identified:<br><br>**Information Security Policy**<br><br>• This policy did not have any real substance and appeared prematurely published. The phrase "will be" was frequently used within the document that gave the impression that these standards were not currently implemented, leading to the policy potentially being ineffective.<br><br>• Supporting standards should have been ready/in place by the time this overarching policy was produced. However, of the 20 supporting documents listed in the appendix, 13 were noted as current with eight of these as the responsibility of IT. Six of the eight documents were provided for review.<br><br>**Information Security Acceptable Use of Information Assets**<br><br>• A supporting policy should provide the guidance for the specific area it covers however this example contained multiple redirections to other documents and lacked the detail required.<br><br>• The Key Points in section 2.2 could lead users to look to this area for guidance rather than find the detail within the policy and also inadvertently dismisses other areas of policy that are not considered “key”.<br><br>• Users were redirected to other documents multiple times. The Council should understand and define the overarching policy and supporting standards they require and map the guidance appropriately to avoid crossover and repetition. An example of this would be that users looking for information on Email and Internet acceptable use would first look at the overarching Information Security policy which would redirect them to the Acceptable Use Policy which then redirects again to a separate Email and Internet Acceptable Use policy.<br><br>• Section 3.6 states “*Users of Barrow Borough Council resources have no expectation of personal privacy*” however employees have a human right to a private and family life, both in and out of the workplace, due to the European Convention on Human Rights. |

| | |
|---|---|
| **Rationale (continued)** | • Within section 3.7.3, it would be helpful to clarify that the clear desk policy also applies to when the desk is left unattended and not just to refer to the end of the day.<br><br>• This supporting policy would be better placed being merged with Information Security Policy to give substance to the overarching policy and minimise the redirections for users.<br><br>**Information Security Incident Reporting and Management Policy**<br><br>• This policy was provided as part of the three sub-policies listed in the ISMS. The latest date on this document is 2012 and therefore would strongly indicate it is out of date and in need of urgent review.<br><br>• The policy did not appear to be in the standard Council format.<br><br>• Section 1.9 required updating as it contains out of date references.<br><br>**BBC Template for System Information Security Requirements**<br><br>• This document is not a policy but could potentially form an appendix of the System Configuration and Management sub-policy.<br><br>• It does not provide any information on who is to complete the template or who would assess it.<br><br>• Although it references IT Infrastructure Standards, there is no guidance on where the user can find these.<br><br>**Information Security Policy Annex - Exceptions to Desktop Policy**<br><br>• This document is dated October 2015 and not in standard Council format and therefore requires review.<br><br>• Exceptions to policy should be avoided to ensure policies are uniform across the organisation. This policy could be incorporated within one of the sub-policies to indicate any additional controls in place, if still required, rather than having a separate exceptions document.<br><br>**Tablet Acceptable Usage Policy for Councillors**<br><br>• This document was very repetitious of the Mobile Device Acceptable Use policy. The Council should consider merging these two documents, adding a section for extra requirements that are applicable to councillors rather than have a separate policy. |

| | |
|---|---|
| **Rationale (continued)** | **IT Services Version Control Guidelines**<br>• This policy did not have an approval date but was produced in the standard Council format. The policy review date on the document had been exceeded and therefore a review is required.<br>**Information Technology Change Control**<br>• The policy stated that “Standard Changes" were out of scope for this policy and gives further guidance to what it considers to be in this category later in the document. However, it is not clear where the user would be able to determine whether a change had been fully documented and tested to be considered standard and how this documentation could be checked.<br>• The section on critical changes could provide more detail on what level of approval is “sufficient” and include that a record should be kept of critical changes and where.<br>• The section referring to the Change Authority did not provide clarity on who or what this was.<br>**IT Infrastructure Standards**<br>• Although the last revision is stated as October 2019, this policy has not been converted to the standard Council format.<br>• The current software and applications have been referred to by name rather than generically which would require this sub-policy to be regularly reviewed to ensure changes are recorded accurately. It should also be considered how much detail is appropriate for a public document while protecting the security of the Council’s IT Infrastructure.<br>**Data Backup Overview**<br>• This document was last dated August 2016 and therefore required review.<br>• The document was provided as supporting documentation to the IT Infrastructure Standards which is in itself a sub-policy of the Information Security Policy. As such, it should be considered whether this is required as a separate document or if it can be merged into the IT Infrastructure Standards. |
| **Response** | The phrase "will be" was frequently used within the document but I think this is a matter of semantics and is attributable to the author’s style of writing rather than weaknesses in the system. We will review to ensure the policies provide clear guidance. |

| | |
|---|---|
| **Response (continued)** | Our view was that the key documents should be published when they are ready rather than wait for all the documents to be in place. IT policies need to be responsive to a changing environment and in many cases changes to a policy can be referenced in other policies retrospectively.<br><br>It is agreed that not all the policies went to Council. We need to make clear distinctions between policies that are created as guidance for end users which will go through the Council process. In addition there will be internal IT Services policies which will be used be qualified staff with a detailed understanding of the Council's systems. These relate to the type and level of access that users have and are supplemented by exception policies. There would be little value in these types of policies going through the Council's process. We will refer to these as protocols but they may contain the word policy because they will include technical interventions which are called policies by the IT community and are used to block or restrict access.<br><br>**Information Security Acceptable Use of Information Assets**<br><br>We will review the wording in sections 2.2, 3.6 3.7 of the Information Security Acceptable Use of Information Assets<br><br>I will review whether this should have been part of the ISMS but as previously stated these policies were developed in line with the advice of third party provider. Their views are likely to be different to the third party providers that were engaged to undertake this audit.<br><br>**Information Security Incident Reporting and Management Policy**<br><br>Agreed that this policy is out of date and will be reviewed as part of the on-going process.<br><br>**BBC Template for System Information Security Requirements**<br><br>We will review where this should sit as part of this process.<br><br>**Information Security Policy Annex - Exceptions to Desktop Policy**<br><br>Agreed that this policy is out of date and will be reviewed as part of the on-going process.<br><br>**Tablet Acceptable Usage Policy for Councillors**<br><br>Agreed IT Services are reviewing the provision of mobile devices for Officers and Members as part of an infrastructure project and this will be considered. |

| | |
|---|---|
| **Response (continued)** | **IT Services Version Control Guidelines**<br><br>Agreed that this policy is out of date and will be reviewed as part of the on-going process.<br><br>**Information Technology Change Control**<br><br>Agreed this will be reviewed as part of the on-going process and the comments will be considered. It should be noted that this policy is internal to IT and will be used be qualified staff with a detailed understanding of the Council's systems<br><br>**IT Infrastructure Standards**<br><br>Agreed this will be reviewed as part of the on-going process and the comments will be considered.<br><br>**Data Backup Overview**<br><br>Agreed this will be reviewed as part of the on-going process and the comments will be considered. It should be noted that this policy is internal to IT and will be used be qualified staff with a detailed understanding of the Council's systems. |

# 3. REJECTED RECOMMENDATIONS

## 3.1 PRIORITY ONE RECOMMENDATIONS

There have been no rejected Priority One recommendations during the reporting period.

## 3.2 PRIORITY TWO RECOMMENDATIONS

There have been no rejected Priority Two recommendations during the reporting period.

# 4. INTERNAL AUDIT COVERAGE:

## APRIL – JULY 2021

| Report Number | Audit Assignment | System Significance Band | Status | Assurance |
|---|---|---|---|---|
| | **ANNUAL AUDITS** | | | |
| 21-01 | Income Collection | 1 | | |
| 21-02 | Housing Benefits | 1 | | |
| 21-03 | Council Tax & Council Tax Support | 1 | Commenced | |
| 21-04 | Business Rates (NNDR) | 1 | Commenced | |
| 21-05 | Risk Management | 1 | | |
| 21-06 | Cash Floats/Receipting Controls | - | | |
| 21-08 | Fraud and Corruption Survey | 2 | | |
| 21-09 | Performance Management | 2 | | |
| 21-10 | Budgetary Control | 2 | | |
| 21-11 | Treasury Management | 2 | | |
| 21-12 | Car Park Meter Income | 2 | | |
| 21-13 | Payroll (incl Expenses) | 2 | Draft Final | Substantial |
| 21-14 | Accounts Receivable | 2 | | |
| 21-16 | Main Accounting System and Periodic Controls | 2 | | |
| 21-17 | Procurement (inc. Ordering) | 2 | Commenced | |
| 21-18 | Accounts Payable | 2 | | |
| 21-19 | Housing Rents | 2 | | |
| 21-20 | Standing Orders/Financial Regs/Council Plans & Policies | 2 | | |
| 21-21 | Housing Maintenance (Day to day repairs) | 2 | | |
| 21-22 | NFI responsibilities | - | Ongoing | N/a |
| 21-24 | Benefit Certification | - | | N/a |
| 21-25 | Business Grant Review | - | In Progress | N/a |
| 21-26 | Substantive Expenditure Testing | - | In Progress | N/a |
| 21-27 | Recruitment - Review | - | Draft | Restricted |
| 21-28 | Arts Council Grant | - | Complete | N/a |
| 21-29 | Covid Grants Post Assurance Work | - | In Progress | N/a |

| Report Number | Audit Assignment | System Significance Band | Status | Assurance |
|---|---|---|---|---|
| | **COMMUNITY ORGANISATIONS AND MAYOR'S ACCOUNT** | | | |
| - | Hawcoat | - | In Progress | N/a |
| - | Abbotsvale | - | | N/a |
| - | Dalton Community Association | - | | N/a |
| 21-23 | Mayor's Account | - | | N/a |
| | | | | |
| | **IT ENVIRONMENT AUDITS** | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **21-07** | **IMPLEMENTATION REVIEW** | | | |
| | Markets | | | |
| | Kennels | | | |
| | | | | |
| | | | | |

**Fraud Hotline Calls**

| | Revenues/ Benefit related | Staff Related | Other | Total |
|---|---|---|---|---|
| 2021/22 (April – July) | 2 | 0 | 12 | **14** |
| 2020/2021 (Full year) | 35 | 1 | 28 | **64** |

# 5. CONTRACT AUDIT

| Report Number | Audit Assignment | Status | Assurance/ Comment |
|---|---|---|---|
| CR119 | Crematorium rebuild | Ongoing | Stages 1-3 findings issued.<br>Further information requested October 2019 |
| CR120 | Building Cleaning | Information awaited | - |
| CR123 | Harding Rise | Ongoing | Stage 1&2 findings issued.<br>Stages 3&4 complete, awaiting Stage 5 |
| CR132 | Portland Walk Car Park Maintenance | Stage 1-2 findings issued | Stages 2 & 3 findings produced. |
| CR133 | Insurance | Information awaited | - |
| CR134 | Public Conveniences – Cleaning contract | Information awaited | - |
| CR135 | Future High Street Consultancy | Information awaited | - |
| CR136 | Forum catering & cleaning | Information awaited | - |
| CR137 | Lift servicing & maintenance | Information awaited | - |
| CR138 | Electrical Installation Testing | Information awaited | - |
| CR139 | Electrical Reactive Maintenance | Information awaited | - |
| | | | |

# 6. CLASSIFICATIONS

## 6.1 Classification of Assurance Levels

At the conclusion of each audit, we give an overall opinion on the level of assurance, which we consider is provided by the controls in place within the system audited. The following classification of assurance levels has been adopted:

| Level | | Definition |
|---|---|---|
| 1. | Unqualified Assurance | The controls appear to be consistently applied. |
| 2. | Substantial Assurance | Evidence was identified to suggest that the level of non-compliance with controls may put some of the system objectives at risk. |
| 3. | Restricted Assurance | The level of non-compliance identified places the system objectives at risk. |
| 4. | None | Significant non-compliance with controls was identified leaving the system vulnerable to error and abuse. |

## 6.2 Priority of Recommendations

Our audit recommendations are categorised by three priority levels: -

*Priority 1* Major issues that we consider need to be brought to the attention of senior management.

*Priority 2* Important issues which should be addressed by management in their area of responsibility.

*Priority 3* Detailed issues of a relatively minor nature.

# 7. PERFORMANCE

The Public Sector Internal Audit Standards (PSIAs) require Internal Audit to be measured in terms of performance. The indicators below provide information over the arrangements and effectiveness of Internal Audit.

| **Indicator** | | **2021/22** |
|---|---|---|
| 1 | Percentage of Draft reports issued within 10 working days of completion of audit fieldwork. | 100% |
| 2 | Percentage of Management Responses received within 20 working days of issue of the Draft report. | 100% |
| 3 | Percentage of Final reports issued within 10 working days of receipt of management response. | 100% |
| 4 | Percentage of Priority 1 and Priority 2 Recommendations acceptable to the audit client. | 100% |

# 8. Draft Reports issued

| **Ref** | **Audit** | **Date issued** |
|---|---|---|
| 20-25 | Covid Risk Assessment – Post Assurance Review | 10 June 2021 |
| 21-27 | Recruitment – Review | 15 June 2021 |
| 21-13 | Payroll | 13 July 2021 |

# APPENDIX 1 – RESTRICTED ASSURANCE AUDITS

| | | Recommendations | | | Previous Recommendations | | | Total | Date Issued |
|---|---|---|---|---|---|---|---|---|---|
| **Ref** | **Audit** | **P1** | **P2** | **P3** | **P1** | **P2** | **P3** | | |
| 20-25 | Covid Risk Assessment – Post Assurance Review (Draft) | 2 | 8 | 1 | | | | **11** | 10 June 2021 |
| 21-27 | Recruitment – Review (Draft) | | 1 | | 3 | 2 | 1 | **7** | 15 June 2021 |