# INTERNAL AUDIT REPORT

| | | | |
|---|---|---|---|
| **FROM:** | Audit and Risk Manager | **SUBJECT:** | ICT Strategies and Policies |
| **TO:** | Head of Customer and Digital Services | **DATE:** | 1 May 2024 |
| **C.C.** | Chief Executive<br>Deputy Chief Executive<br>Head of Finance<br>Portfolio Holder (Cllr J Harrison) | | |

---

## 1 Introduction

1.1 In accordance with the Audit Plan for 2023/24, an examination of the above subject area has recently been completed by Ian Davy, Principal Internal Auditor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

## 2 Background

2.1 Having appropriately designed and executed policies helps to ensure that service areas can undertake their functions appropriately when using ICT based systems and that consistent standards are applied to system management where key responsibilities are devolved to service areas.

## 3 Objectives of the Audit and Coverage of Risks

3.1 Audits of ICT do not tend to follow the 'normal' risk-based approach, with the audit reviewing the management controls in place.

3.2 However, in scoping the audit, the following risks were identified by the auditor and agreed with the Head of Customer and Digital Services:

- Cost to the Council arising from fines in the event of a data breach.
- Financial impact in the event of system instability / unavailability.
- Financial impact of actions taken outside of ICT that would be covered by an ICT policy.
- Lack of adequate security policies may impair legislative action in the event of system misuse.
- Lack of adequate policy compliance for systems which exist outside of the ICT environment.
- Data protection / information security breach.
- Unavailability of systems impacting on service delivery.

- System vulnerabilities exploited allowing fraudulent actions to be undertaken on the systems in place.
- The strategies and policies do not reflect or help achieve the Council's objectives.

3.3 The risks identified above were covered in overview against the following key control areas:

- Strategy and Policy Framework
- Review, Approval and Enforcement, and
- Publishing.

3.4 The work in this area helps the Council to achieve Priority 1 (Delivering valued, sustainable services) of the new Corporate Strategy Warwick District 2030, particularly in relation to the need to ensure that the Council can achieve and demonstrate delivery of high quality services, with specific reference being made to the Digital and Customer Strategy in the ways that this will be delivered.

## 4 Findings

### 4.1 Recommendations from Previous Reports

4.1.1 The current position in respect of the accepted recommendations from the previous audit, reported in October 2019, was reviewed. The current position is as follows:

| Recommendation | | Management Response | Current Status |
|---|---|---|---|
| 1 | The 'Information Security Incident Reporting' policy should be reviewed and updated. | The policy is already under review with target completion date (for adoption) of December 2019. | The version control matrices within the named policies and the Policy Review list provided by the Head of Customer and Digital Services indicate that there were no updates undertaken after the last audit.<br>Only three policies have been updated within the current and previous calendar years.<br>(see 4.3.1 below) |
| 2 | Ongoing work to update data retention, data handling and classification policies should be completed and updated policies should be made available to staff. | The polices are already under review with target completion date (for adoption) of December 2019. | |
| 3 | All remaining policies should be reviewed and updated. | The polices are already under review with target completion date (for adoption) of December 2019. | |

### 4.2 Strategy and Policy Framework

4.2.1 The Head of Customer and Digital Services (HCDS) advised that the Digital Strategy, referred to in the Change Management Programme, was now in place,

as set out in the 'Change Programme – Case for Change' document. This had been approved by Cabinet in March 2024.

4.2.2 He highlighted that the previous strategy, approved as part of the joint working arrangements with Stratford-on-Avon District Council covering 2021 to 2024 was, however, still relevant for the vast majority of what it covered and update reports had previously been presented to Overview and Scrutiny Committee to advise them of progress against specific workstreams covered under it.

4.2.3 He advised that the 'joint' strategy encompassed all of the intended work within a single document. However, the new, one-page, strategy highlights the priorities that are being worked towards but does not go into the detail as to how they will be. He also highlighted that specific initiatives will be identified as part of the Change Programme and aligned to the Council's priorities and objectives accordingly.

**Risk**

**The strategies in place do not align with the Council's objectives and the current Change Programme.**

**Recommendation**

**The detail behind the current Digital Strategy and any sub-strategies required should be drawn up as soon as practicable to support the current change programme, with reference being made to how they align with the Corporate Strategy Warwick District 2030.**

4.2.4 The HCDS advised that the Council would try to work with the ISO27000 principles, although the Council would not go for accreditation as it was not realistic for an organisation of our size to attain. He suggested that, where policies have been revised recently, he had looked to align them to the policies suggested by the appropriate standards.

4.2.5 A list of all of the current ICT policies in place was obtained and, whilst acknowledging that the Council is not going for ISO accreditation, a comparison was undertaken between the policies suggested by ISO and the policies in place at the Council to ensure that the Council's suite of policies was appropriate. On the whole, the policies suggested as being required by the ISO were covered by the policies in place at the Council (although the actual detail included in the policies was not covered).

4.2.6 One specific policy which was not in place was considered to be relevant by the HCDS (Physical Asset Management) and Business Continuity was being reviewed to ensure that 'total cyber security disaster' was planned for. Two others on the ISO list needed to be clarified to ascertain whether they were relevant to the operations at the Council.

**Advisory**

**The 'gaps' between the ISO list of policies and the Council's policies should be reviewed and addressed where considered necessary**.

4.3 **Review, Approval and Enforcement**

4.3.1 The policy list included the dates for when the policies had last been reviewed. This highlighted that the policies in place have, generally, not been reviewed for a number of years. The only exceptions to this are the Identity and Access Management Policy (February 2024), the Patch Management Policy (May 2023) and the Internet Acceptable Usage Policy (February 2023).

4.3.2 All of the policies in place state the required frequency of review. With the exception of the Identity and Access Management Policy, which states that it is to be reviewed 'bi-annually and / or after a security incident', all policies set out that they are due for reviewed 'when deemed appropriate, but no less frequently than every twelve months'.

**Risk**

**Policies cannot be enforced as they are out of date.**

**Recommendation**

**A rolling programme of policy reviews should be implemented, including a review of whether annual reviews are actually required for each policy.**

4.3.3 The HCDS advised that the re-establishment of the ICT Steering Group was due to have been reported to SLT on 21 March 2024. However, this had been deferred due to other corporate priorities but would appear on the agenda for the forthcoming meeting (16 May 2024).

4.3.4 He suggested that the group would cover specific objectives such as the understanding of workload, identification of what is coming forward and the impact of changes on others, with membership being drawn from those 'well placed' within services areas, but not (generally) Heads of Service.

4.3.5 A draft Terms of Reference had been produced and this includes a specific objective regarding policy development.

4.3.6 The HCDS advised that strategies and policies would generally be presented to SLT for sign-off. Upon review of the minutes of the SLT meeting in January 2024, it was confirmed that the Identity and Access Management Policy had been agreed.

4.3.7 Whilst policies receive SLT approval, the HCDS highlighted that, at present, there was no committee sign off of these documents as, whilst Overview and Scrutiny Committee have a role in policy review and development, there is nothing on their current work programme.

4.3.8 The policies currently in place contain a general statement on policy compliance:

Any breach of this policy by staff may lead to disciplinary action being taken and, in cases of gross misconduct, termination of employment without notice. Some cases may result in the Council informing the police and criminal action

may follow. For Members, references in this policy to disciplinary action will mean referral to the Standards Committee and this document will be treated as a local protocol for this purpose. Any breach of this policy by suppliers will be subject to appropriate action by the relevant Deputy Chief Executive. Should the Council be sued due to misuse of Council ICT equipment or the actions of a user which contravene this policy, the Council reserves the right to claim damages from the authorised user concerned.

4.3.9 There is a specific System Lockdown Policy in place that sets out how the Council's computer resources are secured through:

- Standard Build Process
- Drive Encryption
- Group Policy
- Blocking of USB Storage Devices
- Local Administrator permissions
- Network Access permissions
- Mobile Devices (both Council-owned and personal)
- Asset Management
- Anti-Virus.

4.3.10 The HCDS suggested that the next reviews of the policies would cover a review of compliance with regards to how it would be undertaken.

4.3.11 Compliance with some of the policies is already monitored, logged and reported by ICT staff, using specific systems. The Desktop Services Manager provided an overview of the process for monitoring web access which is proactively monitored and also the email acceptable usage which is reactively assessed if a request is received for the email to be released.

## 4.4 Publishing

4.4.1 As highlighted in 4.2.1 above, the One-Page Digital Strategy, included within the Change Management Programme, is now in place and is set out in the 'Change Programme – Case for Change' document.

4.4.2 However, a search for Digital Strategy on the intranet did not bring up any (relevant) results (as it was included within the other document) and the internet had a link only to the previous (2015-19) strategy.

**Risk**

**Staff are unaware of the Council's Digital Strategy.**

**Recommendation**

**It should be ensured that the new strategy is published as a distinct document on the internet and intranet.**

4.4.3 The Policy list referred to above sets out which of the policies are published on the intranet and which are held on the ICT SharePoint folder. The HCDS advised

that the ones not published were only relevant to ICT staff, so there was no intention to publish these to a wider audience through a general intranet page.

## 5 Summary and Conclusions

5.1 Following our review, in overall terms we can give a MODERATE degree of assurance that the systems and controls in place in respect of ICT Strategies and Policies are appropriate and are working effectively to help mitigate and control the identified risks.

5.2 The assurance bands are shown below:

| Level of Assurance | Definition |
|---|---|
| Substantial | There is a sound system of control in place and compliance with the key controls. |
| Moderate | Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls. |
| Limited | The system of control is generally weak and there is non-compliance with controls that do exist. |

5.3 The level of assurance awarded is based on there being a number of issues that were identified requiring further action:

- The detail behind the new 'one-page' Digital Strategy and the supporting strategies are not yet in place.
- The majority of ICT policies have not been formally reviewed for a number of years.
- The latest strategy was not readily identifiable on the intranet.

5.4 A further, relatively minor, 'issue' was identified where an advisory note has been reported. In this instance, no formal recommendation is thought to be warranted and addressing this issue is discretionary on the part of the service.

## 6 Management Action

6.1 The recommendation arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

Richard Barr
Audit and Risk Manager

**Appendix A**

**Action Plan**

**Internal Audit of ICT Strategies and Policies – March 2024**

| Report Ref. | Risk | Recommendation | Rating* | Responsible Officer(s) | Management Response | Target Date |
|---|---|---|---|---|---|---|
| 4.2.3 | The strategies in place do not align with the Council's objectives and the current Change Programme. | The detail behind the current Digital Strategy and any sub-strategies required should be drawn up as soon as practicable to support the current change programme, with reference being made to how they align with the Corporate Strategy Warwick District 2030. | Medium | Head of Customer and Digital Services | Work is underway to develop the content of the Digital Strategy objectives based on the one-page digital strategy outlined as part of the Change Programme. These will be published and made available to staff as soon as possible and identify how they align to both the change programme and the Council's wider corporate objectives. | 31/07/24 |
| 4.3.2 | Policies cannot be enforced as they are out of date. | A rolling programme of policy reviews should be implemented, including a review of whether annual reviews are actually required for each policy. | High | Head of Customer and Digital Services | Work toward a rolling programme to review all ICT Policies was underway at the time the audit was undertaken and will be actioned over the next twelve months.<br>Priority will be given to user facing policies or those which are identified as being deficient through other forthcoming audit reviews.<br>Please note, there are a lot of ICT policies which require review and as such, the target date for completion has been set to provide a realistic timeframe when | 01/05/25 |

| Report Ref. | Risk | Recommendation | Rating* | Responsible Officer(s) | Management Response | Target Date |
|---|---|---|---|---|---|---|
| | | | | | considering the services other ongoing commitments and workload. | |
| 4.4.2 | Staff are unaware of the Council's Digital Strategy. | It should be ensured that the new strategy is published as a distinct document on the internet and intranet. | Low | Head of Customer and Digital Services | Revised materials will be published accordingly and consideration can also be given as to the most appropriate way of communicating the strategy, alongside the wider change programme.<br>Target date set to match the outcomes identified in recommendation 4.2.3. | 31/07/24 |

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High: Issue of significant importance requiring urgent attention.
Medium: Issue of moderate importance requiring prompt attention.
Low: Issue of minor importance requiring attention.