| ISLE OF ANGLESEY COUNTY COUNCIL | |
|---|---|
| COMMITTEE: | AUDIT COMMITTEE |
| DATE: | 12 DECEMBER 2012 |
| TITLE OF REPORT: | PROGRESS REPORT ON INTERNAL AUDIT 01 APRIL 2012 – 16 NOVEMBER 2012 |
| PURPOSE OF REPORT: | FOR INFORMATION |
| REPORT BY: | AUDIT MANAGER - RSM TENON |
| ACTION: | Decisions / approval as detailed in report |

## 1. INTRODUCTION

**1.1** The Operational Plan for 2012-13 was agreed by the Audit Committee at its meeting held on 24 May 2012. The Plan was produced in consultation with the External Auditor, the Section 151 Officer and various meetings and communications with Heads of Service.

**1.2** The following report summarises the work of the Internal Audit Section up to the 16 November 2012 and gives a summary for each of the final reports issued. Executive Summaries of reports issued with a 'Red Assurance' opinion are also provided.

**1.3** Final reports which result in a 'Red Assurance' opinion will be subject to a Follow Up review which will include an audit opinion on the progress of management in implementing the recommendations categorised as High and Medium within the original final report. The results of the Follow Up review will be presented to the next Audit Committee.

**1.4** There were two reviews in the period which resulted in a 'Red Assurance' opinion. The Executive Summaries for these reports are provided at Appendix B and C of this report. Five reviews relating to Information Governance, Information Management and Data Security issues have been undertaken by PWC, WAO and Internal Audit in the past twelve months including these two reports. As a number of the findings and recommendations from these reports are of a similar nature it is considered that the reports are best addressed as a whole rather than individually. Therefore the recommendations from all these reports have been collated into a single action plan which is being addressed by an Information Management Group chaired by the Interim Head of Function – Resources. Progress by the Information Management Group will be reported to the next Audit Committee.

**1.5** The Internal Audit Service uses a Risk Based approach wherever possible but may use System Based, Key Controls, Establishment or Advisory reviews where these approaches are more appropriate.

**1.6** The individual final reports are available to members of this Committee, in confidence, on request to the Head of Service – Audit.

## 2. REPORTS ISSUED TO DATE AND WORK IN PROGRESS (WIP)

**2.1** Table 1 below shows the status of the reviews currently in progress and / or having been completed to final report in this period along with the overall audit opinion.

**Table 1**

| Review Title | Service Area | IA Plan Year | Status | RAG Opinion |
|---|---|---|---|---|
| *Risk Based / System Reviews* | | | | |
| Data Security | ICT/Legal | 2012/13 | FINAL | RED |
| Oriel | Leisure | 2012/13 | FINAL | GREEN/AMBER |
| Modern Records Management | Lifelong | 2012/13 | FINAL | RED |
| BMU Procurement | Housing | 2012/13 | FINAL | Advisory |
| Carbon Targets and Energy Efficiency | Property | 2012/12 | FINAL | GREEN |
| Follow Up – School Recommendations | Education | 2012/13 | FINAL | Little Progress |
| Members' Allowances | Corporate | 2012/13 | WIP | |
| Direct Payments – Soc Services | Social Services | 2012/13 | WIP | |
| School Transport | Transportation | 2012/13 | WIP | |
| Maritime - Income | Highways | 2012/13 | WIP | |
| National Fraud Initiative | Corporate | 2012/13 | WIP | |
| Risk Management - Implemenation | Corporate | 2012/13 | WIP | |
| Council Tax | Finance | 2012/13 | WIP | |
| National Non Domestic Rates | Finance | 2012/13 | WIP | |
| Housing Benefit | Finance | 2012/13 | WIP | |
| Payroll and Overtime | Finance | 2012/13 | WIP | |
| Creditors | Finance | 2012/13 | WIP | |
| Corporate Procurement | Corporate | 2012/13 | WIP | |
| Budget Setting & Monitoring | Corporate | 2012/13 | WIP | |
| *Schools* | | | | |
| Ysgol Rhosybol | Education | 2012/13 | FINAL | GREEN/AMBER |
| Ysgol Bodffordd | Education | 2012/13 | DRAFT | |
| *Referrals* | | | | |

| | | | |
|---|---|---|---|
| Report 09 12-13 | Education | 2011/12 | FINAL |
| Report 10 12-13 | Transportation | 2012/13 | FINAL |
| Report 11 12-13 | Leisure | 2012/13 | FINAL |

## 2.2 Key Findings from Reports Issued

**2.2.1 Data Security** - An audit of Data Security was undertaken as part of the approved internal audit periodic plan for 2012/13. Data Security is the practice of keeping data protected from corruption and unauthorised access. The focus behind data security is to ensure privacy while protecting personal or corporate data.

A key aim of electronic government is for customers to provide personal details possibly via the web, to unlock a set of services sourced from a series of different providers. This is what councils and other government agencies strive to achieve. However, for this to happen requires the confidence of customers that their data is collected, stored, accessed, used and disposed of securely. This requires the effective use and exchange of information both within councils and between councils and other services such as Health and Education. It is therefore crucial that the public has confidence that any data provided is treated with appropriate confidentiality and kept safe from any risk of misuse.

Recent reported losses of personal data such as that from Her Majesty's Revenue and Customs require that all public bodies act to bolster public trust and confidence in the way personal information is handled and kept safe.

The review found that there were a number of weaknesses in the control framework around data security. The main findings from the review were:

**Design of control framework**

- The Council has not nominated a Senior Information Risk Owner and Information Asset Owners as required by the Local Government Data Handling Guidelines.
- The Council has not produced an Information Management Policy.
- The Council has not provided adequate resources and support to strengthen its information governance arrangements in line with findings and recommendations made by the Welsh Audit Office, the Council's External Auditors and Internal Audit.
- There is no contract in place for the disposal of confidential waste and current arrangements were found to have weak internal control.

**Application of and compliance with control framework**

- Controls over the granting and removing of logical access to the Council's network for starters and leavers were found to be weak in relation to the communication of new starter and leaver information between Services and ICT.

The review resulted in two High, fifteen Medium and two Low category recommendations being made and in an overall Red audit opinion.

Additional information on the results of this review can be found in the Executive Summary of this report at Appendix B.

**2.2.2 Oriel Ynys Môn** – An audit of the financial arrangements within Oriel Ynys Môn was undertaken as part of the approved internal audit periodic plan for 2012/13. The Oriel has a gallery shop and cafeteria and records show that visitor numbers for the year ending 31 March 2012 were 98 106. The net running costs for the Oriel for 2011/12 (expenditure less income – including £250k income from the Isle of Anglesey Trust) was £243k which was £33k over budget for the year.

For accounting purposes the market value of the main artwork collections held at the Oriel as at 19 March 2012 is shown in the Asset Register as £1.4m.

Oriel Ynys Môn's collections management procedures are consistent with the Museums Accreditation Standards, which is supervised in Wales by CyMAL (Museums, Libraries and Archives Wales).

The main findings from the review were:

**Design of control framework**

- At the time of the review Oriel Ynys Môn was in the process of bringing together elements of existing policy and procedure into a comprehensive Collections Management Plan.

- The Oriel is also in the process of introducing a formal stock control system. This will decrease the risk that stock items cannot be adequately accounted for in between annual stock checks.

- The current procedure for the reconciliation of the daily takings requires the weekly totals for income collected and the signing of the banking record to ensure that all income is banked intact to be undertaken by a single officer. This increases the risk of irregularity and error in relation to the income collected and that banked.

**Application of and compliance with control framework**

- Although the majority of the of the Oriel's collections of artwork were found to be documented examples of non-documentation in relation to two small collections were identified from testing.

The review resulted in one High, two Medium and eight Low category recommendations being made and in an overall GREEN / AMBER audit opinion.

**2.2.3 Modern Records Management** – An audit of the arrangements for Modern Records Management was undertaken as part of the approved internal audit periodic plan for 2012/13. The review was partly based on the Isle of Anglesey County Council's compliance with records management recommended practices and International Organisation for Standardisation standards (ISO 15489-1:2001). It should be emphasised that the review was concerned with the Council's approach and practices in relation to Modern Records Management and not a review of the new Anglesey Archives facility per se; although the review for completeness included these arrangements.

Records Management is the practice of applying systematic controls to recorded information required in the operation of a business during the various stages of their life cycle: from their creation or receipt, through their processing, distribution, maintenance and use, to their ultimate disposal. The purpose of records management is to promote efficiencies in record keeping, to assure that useless records are appropriately and systematically destroyed while valuable / useful information is protected and maintained in a manner that facilitates its access and use.

The main findings from the review were:

- **Design of control framework**
- The Council has not produced a Records Management Policy setting out the commitment of the Council to manage records in a systematic manner and to ensure accountability and effective practice throughout the Council.
- The Council has not allocated resources or a budget for records management practices such as the transfer and disposal of records. However it was identified through the reported costs associated with transferring and processing the records to the former Ysgol y Graig and Anglesey Archives since September 2011 that the Council spends thousands of pound annually on the transfer of the records to storage and the disposal of confidential waste.
- The Council has published two retention schedules on the Council's intranet which are conflicting. The Council has not formally adopted either retention policy.
- The Council has limited capacity for relocating and for the transfer of records currently stored in the former Ysgol y Graig to the Anglesey Archives.
- Arrangements for the collection and transfer of the modern records to the storage facilities have not been formalised. There is no formal agreement with the current contractor to provide secure transfer.
- Arrangements for the collection and disposal of confidential waste have not been formalised. There is no formal agreement with the current contractor for the collection and disposal of confidential waste or any requirement for proof of disposal of such waste.

**Application of and compliance with control framework**

- Current storage arrangements for the Council's modern records outside of the Anglesey Archives are not adequately secure and do not allow for the convenient retrieval of files and / or documents when required.
- It was found that documents and files were being stored beyond their required retention periods. There is a lack of procedures within some services to identify documents that no longer need to be stored and to arrange for their secure disposal. This puts additional unnecessary pressure on already limited storage facilities.
- Where the relevant information is of a personal or sensitive nature and is no longer required for the purpose for which it was collected, continued storage is in breach of the Data Protection Act (Principle 5), which states that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'
- Following the review of two suppliers used for the transfer and disposal of records management, it was seen that the Council has procured work on an ad hoc basis and has not followed the Council's Procedure Rules in relation to the corporate aggregate spend. By not aggregating spend the Council may also be spending in excess of the threshold where EU procurement regulations apply.

The review resulted in three High and nine Medium category recommendations being made and in an overall Red audit opinion.

Additional information on the results of this review can be found in the Executive Summary of this report at Appendix C.

**2.2.4 Building Maintenance Unit (BMU) Procurement** – An audit of Building Maintenance Unit Procurement arrangements was undertaken as part of the approved Internal Audit periodic plan for 2012/13. The review looked at the arrangements in place within the BMU to procure both goods and services.

The review was limited to the BMU's arrangements to ensure compliance with International, National and local procurement directives and especially with the Council's Contract Procedure Rules. Contract Procedure Rules form part of the Council's Constitution and are included at section 4.9 of that document.

Section 4.9.1.3 of the Contract Procedure Rules states that the Rules apply to all 'contracts entered into by or on behalf of the Council and the procedures to be followed by employees of the Council.' Section 4.9.1.5 of the Contract Procedure Rules states that 'contracts' refers to all arrangements made by or on behalf of the Council for the provision or supply of goods, intellectual property, work or services, whether paid for in money or otherwise.' Section 4.9.1.7 of the Rules states that 'the Rules are mandatory requirements.'

The general principles of the Contract Procedure Rules are stated as including:

- Section 4.9.2.1.1 – 'to aim for the best outcome possible for the Council and the people it serves, having regard to the resources available;
- Section 4.9.2.1.2 – 'to ensure that the result is untainted by consideration of benefit to any individual involved in the exercise, or the suspicion of it'; and
- Section 4.9.2.1.3 – 'to ensure compliance with all applicable legislation.'

In 2011/12 the Building Maintenance Unit (BMU) expenditure with external suppliers was £2.55M based on ledger cost code records for codes P0001 to P0999.

Conclusions from Review - The review concluded that the BMU has arrangements in place in relation to the procurement of goods which include discounts negotiated with suppliers of goods and arrangements with sub-contractors based on set hourly rates. The BMU believe that such arrangements are providing value for money for the Council.

However, the review found that the BMU had no procedures in place to ensure that procurement undertaken by the BMU was in line with the Council's Contract Procedure and Financial Procedure Rules. The lack of such procedures was reflected in Audit testing which found that within the samples of goods and services with a combined value of over £30k procured by the BMU there was no evidence of compliance with Contract Procedure Rules in relation to tendering and contracts.

The reason for non compliance with Council CPRs should be investigated to determine if there are any exceptional circumstances of the procurement requirements of the BMU which mean that current CPRs and FPRs are inappropriate or impractical in providing procurement methods that provide value for money.

Internal Audit is to issue a report on Corporate Procurement Arrangements which partly explains a number of the weaknesses found in the BMU arrangements which, we understand are reliant on corporate arrangements. The Corporate Procurement Arrangements report should therefore be read in conjunction with this report.

NB – This review did not include testing of whether value for money was, or was not, being achieved by the BMU via procurement but only whether such procurement complied with International, National and Council procurement directives.

This was an advisory review for which a formal audit opinion is not applicable.

**2.2.5 Carbon Targets and Energy Efficiency – (Corporate Risk Reference YM6) -** A review of arrangements in relation to Carbon Targets and Energy Efficiency was undertaken as part of the approved Internal Audit periodic plan for 2012/13. The Carbon Reduction Commitment is a mandatory cap and trade emissions scheme designed to reduce the volume of $CO_2$ emitted in the UK and promote improvements in energy efficiency.

The scheme was launched in April 2010. Organisations qualify as participants in the scheme based on their electricity usage. An organisation qualifies as a full participant if it has at least one half hourly electricity meter (HHM) and consumed over 6k megawatt-hours (MWh) over the 2008 qualifying year. Full participants are required to monitor their $CO_2$ emissions and to purchase allowances, which were initially quoted at a price of £12 per tonne of $CO_2$. From April 2011 participating organisations have been required to buy $CO_2$ allowances based on their previous years' emissions.

This review was conducted to ascertain what mitigating actions are in place to reduce the risk of not meeting Carbon Reduction Targets, to ensure that the mitigating actions are in place, consistently applied and effective in mitigating the stated risk.

The review found that in fact the Council does not qualify to be a full participant in the Carbon Reduction Commitment Scheme and that therefore the risk can be removed from the Corporate Risk Register.

The main findings from the review were:

**Design of control framework**

- The review found that controls within this area were suitable designed to allow for the recording and monitoring of $CO_2$ emissions by the Council and in determining the position of the Council in relation to joining the Carbon Commitment Scheme.

**Application of and compliance with control framework**

- Minor issues only were identified in relation to the on-going process of entering paper bills onto the DYNAMAT system to maximise the potential from the system and to produce reports.

The review resulted in one Low category recommendation being made and in an overall GREEN audit opinion.

**Schools Audits –** The objective of the review of schools is to provide assurance on the operation, effectiveness and adequacy of key internal controls relating to income and expenditure systems, financial and budgetary management and governance arrangements within the school. The following school reviews were completed to final report stage during the period covered by this report:

**2.2.6 Follow Up School Recommendations -** As part of the approved Internal Audit periodic plan for 2012/13 we have undertaken a review to follow up progress made by the Isle Anglesey County Council's schools to implement previous internal audit recommendations. The recommendations considered as part of the follow up review were from reports relating to the following schools:

- Ysgol Moelfre;
- Ysgol Rhosneigr;
- Ysgol Goronwy Owen;
- Ysgol Bryngwran;
- Ysgol Beaumaris;
- Ysgol Llanfairpwll; and
- Ysgol Uwchradd Bodedern.

Of the 37 recommendations considered in this review 8 were classified as 'Medium' and 29 as 'Low' category recommendations. There were no 'High' recommendations relating to this review.

The Auditor visited all the schools and interviewed the Head Teachers responsible for the implementation of recommendations to determine the status of agreed actions. Where appropriate, audit testing has been completed to assess the level of compliance with this status and the controls in place.

This is an advisory report to Education management on the progress in implementing Internal Audit recommendations by schools. Individual schools have been sent action plans detailing the outstanding recommendations and requested to provide updates on implementation to Internal Audit for update on 4Action.

Conclusions from review - Taking account of the issues identified in the report in our opinion management has demonstrated 'little progress' in implementing actions agreed to address internal audit recommendations.

We understand that the Education Service has on going arrangements in place to follow up Internal Audit recommendations. However, the review found that the schools included in the review have made unsatisfactory progress in implementing recommendations.

Head Teachers should be reminded of the need to respond promptly to regulatory reports, including those from Internal Audit, to ensure that weaknesses in internal controls are addressed and identified risks appropriately mitigated.

We have reiterated recommendations where these have not yet been implemented. In addition, we have made new recommendations where appropriate; these are detailed in the findings section of the report.

This was a Follow Up review which resulted in an overall opinion that 'little progress' has been made in implementing these recommendations relating to schools.

**2.2.7 Ysgol Rhosybol –** Ysgol Rhosybol is a rural Primary school of approximately 55 pupils. A new Head Teacher was appointed to the school in January 2011. The main findings from the review related to the following identified weaknesses in internal control;

- Policies were in place to support the corporate governance framework. It was found however that the minutes of the Board of Governors' meetings were not sufficiently complete and detailed to allow transparency and compliance with the Government of Maintained Schools (Wales) Regulations 2005.
- Testing undertaken at the school identified some weaknesses in the operation of the procedures relating to ordering goods, works and services; orders were not routinely completed in advance of the purchase.
- It appeared that complete and accurate records were maintained in relation to school lettings and the correct procedures followed when letting the premises; some instances were identified however where there was no lettings agreement form completed for the let and other instances identified where the hirer had not signed the agreement form.

The review resulted in an overall GREEN / AMBER audit opinion.

**2.3 Summary of Outcomes of Reports Issued to Date** – since the 01 April 2012 we have issued two final reports from the Internal Audit Operational Plan 2011-12; seventeen from the 2012-13 plan and eleven referral reports. To date a total of thirty Final reports has been issued in 2012/13.

A summary of the grades given for the final reports issued is shown in the table below. The summary of grades issued is as follows:

| RAG Opinion / Grade | What is meant by the RAG Opinion / Grade | Since Last Audit Committee In Period | April to Nov 2012 |
|---|---|---|---|
| Green (A&B Grade) | Taking account of the issues identified, the Authority can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective. | 1 | 3 |
| Green Amber (C Grade) | Taking account of the issues identified, the Authority can take reasonable assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.<br>However we have identified issues that, if not addressed, increase the likelihood of the risk materialising. | 2 | 5 |
| Red Amber (D Grade) | Taking account of the issues identified, whilst the Authority can take some assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective, action needs to be taken to ensure this risk is managed. | 1<br>(Little Progress) | 2 |
| Red (E Grade) | Taking account of the issues identified, the Authority cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.<br>Action needs to be taken to ensure this risk is managed. | 2 | 3 |
| Advisory / Investigation | Advisory review designed to provide best practice advice – No formal opinion. | 4 | 17 |
| | **Total** | **10** | **30** |

## 3 PERFORMANCE AGAINST TARGETS FOR PERIOD 01/04/12 – 16/11/12

**3.1** The table below shows the Internal Audit Service's performance against agreed targets set out in the Service's Delivery Plan for 2012/13. Reporting progress against these targets is also made to the Quarterly Performance Meetings for Finance.

| Performance Measure | Target 2012/13 | Actual Adjusted for Period* | Target Status | Direction of Travel since previous period |
|---|---|---|---|---|
| % of audit reviews completed to draft in year (63 reviews in plan – 1 to Draft in period & 17 Finals– excluding referrals) | 90% | 46% | ☹ | ⬇ |
| Overall customer satisfaction levels from questionnaires | 90% | 100% | ☺ | ⬅➡ |
| % of High & Medium IA recommendations implemented – from 01-04-10 | 80% | 67% | ☹ | ⬇ |
| Number of planned reviews of Identified High Corporate Risk Areas | 8 | 3 | 😐 | ⬆ |
| Two Audit Committee Training Sessions in period | 2 | 2 | ☺ | ⬆ |

**3.2** The percentage of Audit Plan completed figure at 46% is below the target of 90%. This is mainly due to the eleven referrals that have been completed and reported on in the period diverting resources from the planned Internal Audit work. An on-going investigation has taken up much of an FTE Auditor's time during the first seven months of this year. This investigation has now been referred to the Police.

The period has also seen a disproportionate amount of annual leave being taken in the summer months.

**3.3** The percentage of High and Medium categorised recommendations implemented is below target at 67%. Internal Audit will continue to send out reminders to update in order to ensure that all actions on recommendations are recorded on the system.

## 4. REFERRALS

**4.1** During the course of the year the Internal Audit Section is required to carry out work on matters which come to light during the programmed audit work, or matters which are brought to its attention by other Departments, or work which other Departments request the Internal Audit Section to carry out. Work may also be requested by the External Auditor to provide information or to assist in the provision of information. Some of these referrals result in the issue of formal audit reports whilst others may not (e.g. the allegation / information is found to be incorrect and therefore there is nothing to report, or the amount of work is not sufficient to warrant a full audit report or the matter is covered by an External Auditor's report).

**4.2** Eleven reports relating to referrals have been issued in 2012/13 to date. Three of these have been reported on in the period covered by this report (Referral Reports 09; 10 and 11).

**4.3** Report 09 related to incidences of late banking of income and resulted in the resignation of the staff member involved. A Final report for decision as to further action was reported to the Interim Section 151 Officer and to the Monitoring Officer.

**4.4** Report 10 related to a referral concerning the tendering of Taxi services and a report was issued concluding that there was no evidence of irregularity on the routes subject to the referral.

**4.5** Report 11 related to the collection of outstanding debts in relation to hires of at a Council Leisure Centre.

## 5. RECOMMENDATION TRACKING

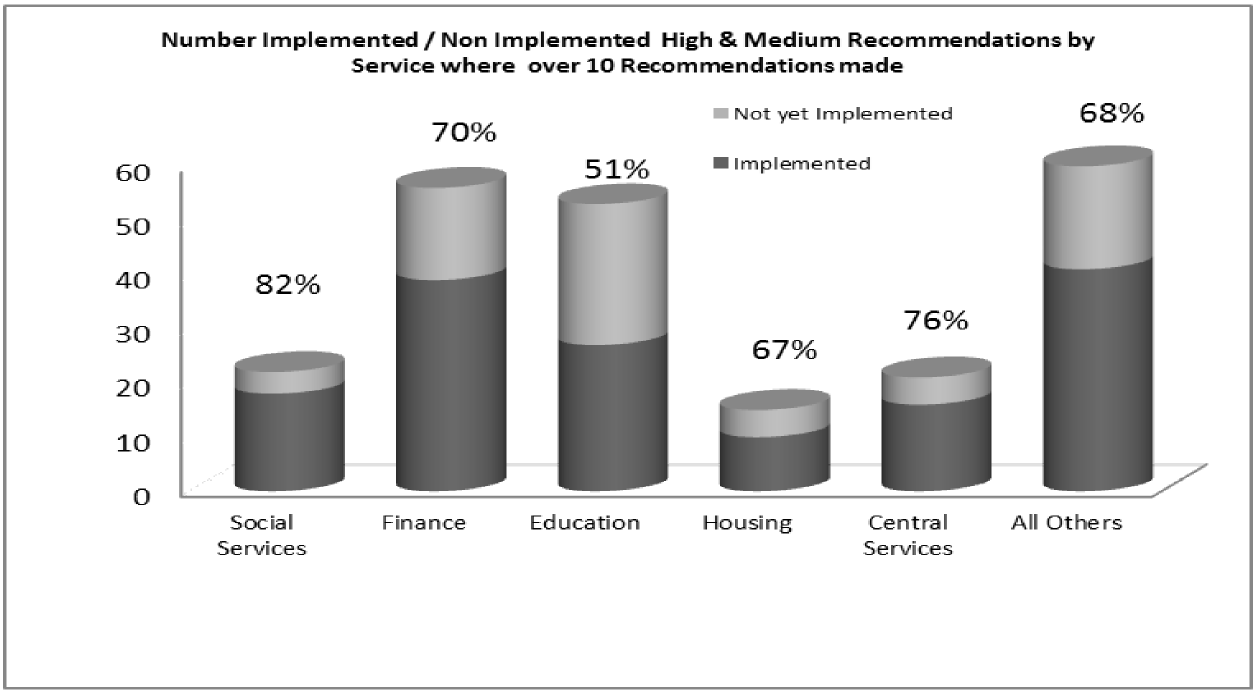
**5.1** For reporting to this Committee only recommendations made since 01-04-2010 have been included in the recommendation tracking analysis.

**5.3** The performance in implementing recommendations in the period is below target with 67% of High and Medium recommendations having been recorded as implemented. A graph showing the breakdown of recommendation implementation by Service is provided at Appendix A.

**AUDIT MANAGER**
**12 December 2012**

**APPENDIX A**

**Recommendation Tracking Table – All Recommendations Created Since 01-04-2010**
**Progress Table:** % implemented / non implemented of high and medium category recommendations by service where over 10 recommendations made.



In our opinion therefore based on the self assessed data in the Progress Table above the Council has made **'adequate progress'** in the period in implementing High and Medium categorised Internal Audit recommendations. This is based on the percentage of recommendations (excluding those that have not yet reached their agreed implementation date) for which the self assessed status is either, implemented or superseded, which total at the end of the period was **67%** of all such recommendations.

**APPENDIX B**

**Red Assurance Reports**

## Data Security – Report Ref: 1787.12/13

# 1 EXECUTIVE SUMMARY

### 1.1 INTRODUCTION

An audit of Data Security was undertaken as part of the approved internal audit periodic plan for 2012/13. Data security is the practice of keeping data protected from corruption and unauthorised access. The focus behind data security is to ensure privacy while protecting personal or corporate data.

A key aim of electronic government is for customers to provide personal details possibly via the web, to unlock a set of services sourced from a series of different providers. This is what councils and other government agencies strive to achieve. However, for this to happen requires the confidence of customers that their data is collected, stored, accessed, used and disposed of securely. This requires the effective use and exchange of information both within councils and between councils and other services such as Health and Education. It is therefore crucial that the public has confidence that any data provided is treated with appropriate confidentiality and kept safe from any risk of misuse.

Recent reported losses of personal data such as that from Her Majesty's Revenue and Customs require that all public bodies act to bolster public trust and confidence in the way personal information is handled and kept safe.

The Local Government Data Handling Guidelines produced by the Welsh Local Government Association, Local Government Association, SOCitm and SOLACE are designed as a response to that need for customer confidence. The Guidelines set out the fundamental steps that every council should take to mitigate the ever present risk that personal information is lost or that data protection systems fail. They therefore provide chief executives, senior managers and elected members with a vital aid in discharging their responsibilities and accountability for secure and effective handling of personal information.

The Information Commissioner, Richard Thomas in his introduction to the Guidelines in November 2008 stated that:

'I believe that if councils effectively implement the steps set out in the guidelines, they will significantly reduce the risk of incidents and problems, and in doing so, help build the necessary public trust in the handling of personal information that recent and well publicized incidents can only have eroded.'

This audit has reviewed the Isle of Anglesey County Council's compliance with selected key elements of the Guidelines and found non-compliance in a number of these key areas. Some of these weaknesses have already been reported on by the Welsh Audit Office in its 'Information Management Review Feedback Report' published in March 2012 and the Council's External Auditors' 'Does the Council have suitable arrangements for the effective governance of its information?' report published in May 2011.

It is intended that following the publication of Internal Audit's reports on Data Security, Records Management and Business Continuity, a consolidated action plan incorporating all related recommendations including those of the WAO and External Auditor will be produced.

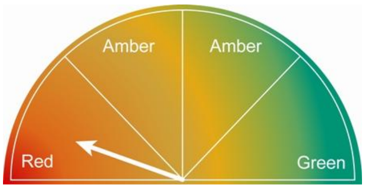
The lack of compliance with key Data Security practices amongst staff and members is considered to be a significant risk to the Council's reputation and could result in large fines through unauthorised disclosures of data.

The objectives and main risks considered as part of this audit were as follows:

| | |
|---|---|
| Objective: | The Council has policies and procedures in place to ensure the integrity and security of the electronic and physical data held. |
| Risk: | The Council fails to maintain the security and / or integrity of its electronic and physical data leading to unauthorised access / loss of data and / or non-compliance with Data Protection legislation. |

| | |
|---|---|
| Objective: | The Council complies with the requirements of Local Government Data Handling Guidelines. |
| Risk: | The Council fails to comply with legislation through failure to provide adequate responsibility and accountability for the secure and effective handling of personal information. |

## 1.2 CONCLUSION



**Taking account of the issues identified, the Council cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied or effective.**

**Action needs to be taken to ensure this risk is managed.**

The above conclusions feeding into the overall assurance level are based on the evidence obtained during the review. The key findings from this review are as follows:

### Design of control framework

- The Council has not nominated a Senior Information Risk Owner Officer and Information Asset Owners as required by the Local Government Data Handling Guidelines. Overall accountability for the management and security of the Council's information has therefore not been assigned. The Guidelines require that: '*there should be clear lines of accountability throughout the organisation together with a programme of staff awareness raising, starting at induction but continually updated, which clearly sets out the expectations of staff*.'
- The Council has not produced an Information Management Policy setting out the commitment of the Council to manage information in a professional manner, so as to ensure that the Council's knowledge base is fully and efficiently exploited, whilst providing the necessary accountability and assurance. Therefore staff, Members and the public do not know how the Council manages its information.
- The Council has not produced an Information Charter as required by the Local Government Data Handling Guidelines setting out how the Council handles information and how members of the public can address any concerns that they have.
- Controls over the granting and removing of logical access to the Council's network for starters and leavers were found to be weak in relation to the communication of new starter and leaver information between Services and ICT. Testing found that some leavers' access to the network was still active after the date that the employees had left the employment of the authority.
- There is no procedure in place for the review of the Council's applications which collect and store personal, sensitive and confidential information to ensure that security over those systems meets the requirements of the Council's ICT Security Policy and the Information Security Standards (BS ISO/IEC 27002:2005).
- There are no procedures in place to identify what data is being processed and held by the Council.  Data classification standards have not been defined to specify how sensitive, personal and business confidential data should be handled and transmitted.

- The Council has not undertaken a data mapping exercise to identify and control the key risk areas where information is transferred between itself and other organisations.
- The Council has not implemented a clear desk policy to ensure that staff do not leave documents and / or files containing personal, sensitive or confidential information on their desks unattended. There is an increased risk of unauthorised access to data where cleaning staff have access to offices after the normal staff working hours.
- The Council has not provided data security awareness raising or training sessions to staff. The Local Government Data Handling Guidelines (LGDHG) require that councils: *'ensure awareness raising and training is conducted at the appropriate level and monitor understanding and ability periodically; regular updates should be scheduled for all employees.'*
- The Council does not have formal written procedures for the reporting of data incidents and other information or data security issues. This increases the risk that incidents go unreported to the relevant staff and therefore that no action is taken to ensure that the incident does not reoccur.
- The Council does not have formal written procedures for the recovery from information risk incidents including the Council's media and legal response and the responsibilities of staff dealing with such incidents, including responsibility for reporting to the Information Commissioner's Office as appropriate.
- Arrangements for the collection and disposal of confidential waste have not been formalised. There is no formal agreement with the current contractor for the collection and disposal of confidential waste or any requirement for proof of disposal of such waste. Current informal procedures result in confidential waste sacks being stored insecurely within offices and corridors prior to collection.
- There are no polices in place for the review of data security procedures.
- There is no central inventory / asset register of ICT equipment and therefore no regular check that ICT equipment containing personal, sensitive or confidential data can be accounted for.

### Application of and compliance with control framework

- Current storage arrangements for the Council's modern records are not adequately secure and do not allow for the convenient retrieval of files and / or documents when required. A separate review and report on the management of the Council's Modern Records is being undertaken by Internal Audit.
- The Council has published two separate document retention policies on its Intranet, one from Zurich and one from the Records Management Society of Britain. The Council has not determined which should be adopted by Council staff. A corporate approach to document retention is required if the new Modern Records storage facility is to be utilised effectively.
- In practice it was found that documents and files were being stored beyond their required retention periods. There is a lack of procedures within some services to identify documents that no longer need to be stored and to arrange for their secure disposal. This puts additional unnecessary pressure on already limited storage facilities.
- Where the relevant information is of a personal or sensitive nature and is no longer required for the purpose for which it was collected, continued storage is in breach of Data Protection Act (Principle 5), which states that 'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'
- Security parameters were found not to have been applied to the appropriate Information Security Standards (BS ISO/IEC 27002:2005) or the Council's ICT Security Policy in relation to two Council systems during the review. These systems were the TOREX system for Leisure Centres and the CALM system to be used for recording of Modern Record storage.
- The Council's Main Office building is open for 24 hours a day, seven days a week for staff with access swipe cards. Testing of staff leavers against their swipe card status on the HFX / Win Time system showed that some cards had not been made inactive, therefore those staff could still gain access to the Council's Main Office. Such weaknesses in controls increase the risk of unauthorised access to personal, sensitive or confidential information. The LGDHG require that:

*'all councils should ensure the security of their information through the physical security of their buildings, premises and systems.'*

- Testing of a sample of leavers to network access status found that access status was still active for five out of six leavers tested. This increases the risk of unauthorised access to information and data held.

## 1.3 SCOPE OF THE REVIEW

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. Control activities are put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively. When planning the audit, the following limitations were agreed:

**Limitations to the scope of the audit:**

- The review will take the form of a high level desk-based review of the Council's Data Security arrangements for electronic and physical data.
- The review will include an assessment of the Council's compliance with a selection of key requirements of the SOCITM Local Government Data Handling Guidelines.
- The work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

The approach taken for this audit was a Risk-Based Audit.

**APPENDIX C**

**Red Assurance Reports**

## Modern Records Management – Report Ref: 1808.12/13

# 1 EXECUTIVE SUMMARY

### 1.1 INTRODUCTION

An audit of Modern Records Management was undertaken as part of the approved internal audit periodic plan for 2012/13. The review was partly based on the Isle of Anglesey County Council's compliance with records management recommended practices and International Organisation for Standardisation standards (ISO 15489-1:2001). It should be emphasised that the review was concerned with the Council's approach and practices in relation to Modern Records Management and not a review of the new Anglesey Archives facility per se; although the review for completeness included these arrangements.

Records Management is the practice of applying systematic controls to recorded information required in the operation of a business during the various stages of their life cycle: from their creation or receipt, through their processing, distribution, maintenance and use, to their ultimate disposal. The purpose of records management is to promote efficiencies in record keeping, to assure that useless records are appropriately and systematically destroyed while valuable/useful information is protected and maintained in a manner that facilitates its access and use.

Records Management is often seen as an unnecessary or low priority administrative task that can be performed at the lowest levels; however with new compliance regulations, emphasis on privacy and data protection, records management has become a highly regarded concern within organisations with a greater focus to implement appropriate records retention and destruction schedules.

This review has concentrated solely on the management of paper records and has not included a review of arrangements in place for the management of electronic records.

The audit found that the Council has made a significant amount of investment in the Anglesey Archives facility that is fit for the purpose of records depository, the facility has also been evaluated as the solution to the provision of a depository service for all the Council's semi-current modern records. The facility has already begun to accept records from Services and is concentrating efforts on transferring those records currently at greatest risk due to their present storage arrangements. From September 2011 to the time of the review (September 2012) work between Services and the Anglesey Archives has resulted in the transfer of 500 boxes of modern records to the facility from the following services; Adult Services; Human Resources; Education and the Economic Development Unit. This process has demonstrated that arrangements to provide a site for secure records deposit are effective and appropriate. The intention now is to expand the service to all of the Council's semi-current modern records and this is considered to be significant progress from where the Council was just two years ago.

At present the facility's main service is to provide a place for archived records. The National Archive's approval awarded to Anglesey Archives this year confirms that the building and archive operations meet the requirements of the Standard in respects such as flood and damp prevention, fire protection, storage arrangements, security etc. If Anglesey Archives is to continue to expand services beyond the storage of archives into the storage of all the Council's semi-current records, further appropriate resources and standards need to be employed; for example adequate staffing levels and production of policies on the type of records that can/cannot be accepted at the facility (i.e. all records must be pest and damp free).

However, away from the Anglesey Archives, the audit found non-compliance in a number of key areas of the Council's Modern Records Management arrangements. Some of these weaknesses have already been reported by the Welsh Audit Office in its 'Information Management Review Feedback

Report' published in March 2012 and the Council's External Auditors', 'Does the Council have suitable arrangements for the effective governance of its information?' report published in May 2011.

It is intended that following the publication of Internal Audit's reports on Data Security, Records Management and Business Continuity, a consolidated action plan incorporating all related recommendations including those of the WAO and External Auditor will be produced.

The lack of compliance with key Modern Record Management practices and several breaches to the Data Protection Act amongst staff and members is considered to be a significant risk to the Council's reputation and could result in large fines.

The latest fine from the Information Commissioners Office imposed on a local authority was £250,000 after employee records were found in a supermarket car park recycle bin. The Council had employed an outside company to digitise the records, but failed to seek appropriate guarantees on how the personal data would be kept secure.

The objectives and main risks considered as part of this audit were as follows:

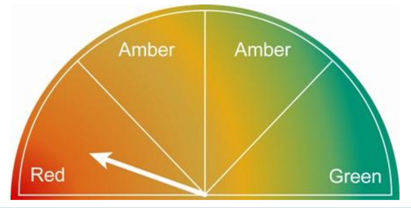
| | |
|---|---|
| Objective | Ensure that appropriate arrangements are in place for management of corporate modern records. |
| Risks | Inadequate modern records management arrangements to ensure the accessibility, security and integrity of corporate records.<br>The records management system/database is not appropriately backed up to ensure that the system can be promptly restored following a disaster scenario. |

| | |
|---|---|
| Objective | Ensure that data stored is secure and cannot be inappropriately accessed or disclosed in relation to Data Protection Act. |
| Risks | Inappropriate accessing and/or disclosure of stored data in breach of Data Protection Act.<br>Unauthorised access to the modern records management database through ineffective logical access controls. |

| | |
|---|---|
| Objective | Arrangements are in place for the secure disposal of stored modern corporate records when they reach the end of their required retention period. |
| Risks | Data is stored unnecessarily incurring storage costs beyond those necessary and creating space issues at the archiving facility.<br>Personal and sensitive data is stored beyond the period for which it was collected in breach of Data Protection Act. |

| | |
|---|---|
| Objective | Departments have adequate procedures and resources in place for the processing of modern records for transfer to Anglesey Archives. |
| Risks | Departments do not transfer modern records to the Anglesey Archives facility due to lack of process and resources;<br>Current inadequate modern records storage arrangements continue. |

## 1.2 CONCLUSION



**Taking account of the issues identified, the Council cannot take assurance that the controls upon which the organisation relies to manage this risk are suitably designed, consistently applied and effective.**

**Action needs to be taken to ensure this risk is managed.**

The above conclusions feeding into the overall assurance level are based on the evidence obtained during the review. The key findings from this review are as follows:

### Design of control framework

- The Council has not produced a Records Management Policy setting out the commitment of the Council to manage records in a systematic manner and to ensure accountability and effective practice throughout the Council. The policy should outline the roles and responsibilities of the services and Anglesey Archives and on a corporate level.
- The Council has not allocated resources or a budget for records management practices such as the transfer and disposal of records. However it was identified through the reported costs associated with transferring and processing the records to the former Ysgol y Graig and Anglesey Archives since September 2011 that the Council spends thousands of pound annually on the transfer of the records to storage and the disposal of confidential waste
- The Council has published two retention schedules on the Council’s intranet which are conflicting. The Council has not formally adopted either retention policy.
- The Council has limited capacity for relocating and the transfer of records currently stored in the former Ysgol y Graig to Anglesey Archives.
- Arrangements for the collection and transfer of the modern records to the storage facilities have not been formalised. There is no formal agreement with the current contractor to provide secure transfer.
- Arrangements for the collection and disposal of confidential waste have not been formalised. There is no formal agreement with the current contractor for the collection and disposal of confidential waste or any requirement for proof of disposal of such waste. Current informal procedures result in confidential waste sacks being stored insecurely within offices and corridors prior to collection.

### Application of and compliance with control framework

- Current storage arrangements for the Council’s modern records are not adequately secure and do not allow for the convenient retrieval of files and / or documents when required.
- It was found that documents and files were being stored beyond their required retention periods. There is a lack of procedures within some services to identify documents that no longer need to be stored and to arrange for their secure disposal. This puts additional unnecessary pressure on already limited storage facilities.
- Where the relevant information is of a personal or sensitive nature and is no longer required for the purpose for which it was collected, continued storage is in breach of the Data Protection Act (Principle 5), which states that ‘Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.’
- Following the review of two suppliers used for the transfer and disposal of records management, it was seen that the Council has procured work on an ad hoc basis and has not followed the Council’s Procedure Rules in relation to the corporate aggregate spend. By not aggregating spend the Council may also be spending in excess of the threshold where EU procurement regulations apply.

## 1.3 SCOPE OF THE REVIEW

To evaluate the adequacy of risk management and control within the system and the extent to which controls have been applied, with a view to providing an opinion. Control activities are put in place to ensure that risks to the achievement of the organisation's objectives are managed effectively. When planning the audit, the following limitations were agreed:

**Limitations to the scope of the audit:**

- The review will concentrate on the Council's approach and practices in relation to Modern Records Management.
- The review will not cover the Council's project for Electronic Records Management.
- The work does not provide any guarantee against material errors, loss or fraud or provide an absolute assurance that material error, loss or fraud does not exist.

The approach taken for this audit was a Risk-Based Audit.

*NB – Archives were not considered as part of this review as a separate review of this area was undertaken by the National Archives which resulted in the formal appointment of 'Anglesey Archives as a place of deposit and to award TNA approval to the service.' (TNA Inspection of Anglesey Archives – July 2012) This appointment was the result of considerable work by Lifelong Learning and any arrangements for further storage must ensure that they meet the same standards to ensure that this achievement is maintained.*