Purpose of report

1. To present Members with the most recent reports from Veritau Ltd, the Authority’s Internal Audit provider.

Strategic Planning Framework

2. The information contained in this report is consistent with the Authority’s approved and adopted strategic planning framework:

- **Existing policies and strategies**
  “each NPA is required to maintain an adequate and effective internal audit…” (Financial Regulations, paragraph 17.1 (iv))
  “The Internal Auditor shall determine the scope of any internal enquiries or investigations” (Financial Regulations, paragraph 17.6)

Internal Audit Reports: Summary

3. The cycle of internal audits for 2012/13 has now been completed, and the reports covering the final series of reviews are attached as a series of *appendices*. Whilst the reports undoubtedly contain a lot of information, they are included here in full to give Members the opportunity of discussing any of the detailed findings further, should they so wish.

4. Each Internal Audit Report contains an opinion over the level of assurance provided by the Authority’s systems, according to one of the following five categories:

   - **High Assurance.** Overall, very good management of risk. An effective control environment appears to be in operation.
   - **Substantial Assurance.** Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
   - **Moderate Assurance.** Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
   - **Limited Assurance.** Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance. Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

5. The assurance categories for each of the 2012/13 internal audits reported here is indicated by a ‘✓’ in the following table; for comparative purposes, the assurance results for internal audits in 2011/12 are included, shown as ‘(✓)’. The results from these two years of internal audit work indicate that a good level of control is being maintained.

<table>
<thead>
<tr>
<th>Internal Audit</th>
<th>Level of Assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Main Accounting / Budgetary</td>
<td>✓</td>
</tr>
<tr>
<td>Cash and Bank</td>
<td>✓</td>
</tr>
<tr>
<td>Income, Cash and Bank</td>
<td>✓ (✓)</td>
</tr>
<tr>
<td>Human Resources / Payroll</td>
<td>✓ (✓)</td>
</tr>
<tr>
<td>Creditors / Purchasing</td>
<td>✓ (✓)</td>
</tr>
<tr>
<td>Computer Audit</td>
<td>✓ (✓)</td>
</tr>
</tbody>
</table>

6. With the introduction of a new Payroll system in 2012, we asked for a one-off audit to confirm that the new systems had been implemented satisfactorily. The report from that audit (from June 2012) recorded the level of assurance as ‘substantial’. Since June 2012, the recommendations in that audit report have been implemented, and the level of assurance has moved to ‘High’ (as noted in the above table). A copy of the earlier report is also included at the front of the appendices, for completeness.

7. Within each Internal Audit Report, the Internal Auditor identifies a priority for each action identified, as noted below. No ‘Priority 1’ actions were identified during the 2012/13 series of internal audits.
   - Priority 1: A fundamental system weakness, which presents material risk to the system objectives and requires urgent attention by management.
   - Priority 2: A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
   - Priority 3: The system objectives are not exposed to significant risk, but the issue merits attention by management.

RECOMMENDATION

8. Members are asked to note this report and the appended Internal Audit reports.

Richard Burnett
Director of Corporate Services
21 March 2013
Background Documents: none
1 Summary

1.1 The agreed audit plan for 2011/12 included an Internal Audit review of the new payroll system at YDNPA. It was agreed to delay this audit to May 2012 and the assignment has recently been completed. Field work started on 24 May 2012 and was completed on 1 June 2012. The audit was carried out in accordance with the specification issued on 10 January 2012.

1.2 It was found that the arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1.3 The main issues arising relate to:
   • Starters and leavers
   • Year end statements
   • Recorded totals for the month of March 2012

1.4 Section two of the report sets out the detailed findings from the review, along with the actions that management have agreed to take.
2 Issues Identified and Management Action Plan

1 Starters and leavers

<table>
<thead>
<tr>
<th>Issue Identified</th>
<th>Risk / Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

All new starters are entered onto the Carval payroll system by the Senior Administrator in Finance with a new employee record being created. Information is directly input onto the system based upon information received from Human Resources on the new starters form.

Likewise all leavers are entered onto the Carval payroll system by the Senior Administrator in Finance based upon information received from Human Resources on the leavers form. There is no independent check undertaken.

It maybe possible for the Carval payroll system to produce a report that could be run on a monthly basis listing all starters and leavers processed for the period. This report could then be saved on the shared drive so that an independent check could be undertaken by Human Resources.

<table>
<thead>
<tr>
<th>Management Action Plan</th>
<th>Action to be Taken</th>
<th>Priority</th>
<th>Responsible Officer</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Head of Finance and Resources</td>
<td>Completed</td>
</tr>
</tbody>
</table>

2 Year end statements

<table>
<thead>
<tr>
<th>Issue Identified</th>
<th>Risk / Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

It was found that the creation of employee year end statements such as P60, P11D and other statements such as P45 has not been tested on the new Carval payroll system.

These statutory forms were produced under contract by NYCC for the 2011/12 financial year and not by the Carval system. This will be addressed by the end of the financial year.

<table>
<thead>
<tr>
<th>Management Action Plan</th>
<th>Action to be Taken</th>
<th>Priority</th>
<th>Responsible Officer</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Head of Finance and Resources</td>
<td>April / May 2013</td>
</tr>
</tbody>
</table>
3 Recorded totals for the month of March 2012

<table>
<thead>
<tr>
<th>Issue Identified</th>
<th>Risk / Potential Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each month a download of the accumulated spend against cost and subjective codes was produced by NYCC. Detail from this was then used to update the YDNPA financial system.</td>
<td>The detail payroll costs may be misclassified, although the amounts involved are unlikely to have been material.</td>
</tr>
<tr>
<td>Testing was carried out to see if the payslips and reconciliation from the Carval system agreed to the download from NYCC. It was found that the download from NYCC was incorrect in its classification of costs.</td>
<td></td>
</tr>
<tr>
<td>Whilst the total payroll costs should be correctly stated, there will have been misclassification in the figures used in the preparation of the management accounts and the year end accounts as a result of the information provided by NYCC.</td>
<td></td>
</tr>
</tbody>
</table>

Management Action Plan

<table>
<thead>
<tr>
<th>Action to be Taken</th>
<th>Priority</th>
<th>Responsible Officer</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 This issue will have been eradicated with the move to internalise the Payroll system.</td>
<td>3</td>
<td>Head of Finance and Resources</td>
<td>Completed</td>
</tr>
</tbody>
</table>
### Overall Audit Opinion

<table>
<thead>
<tr>
<th></th>
<th>P3</th>
<th>P2</th>
<th>P1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

### Findings

- [ ] 0
- [ ] 0
- [ ] 0

Business Unit: Yorkshire Dales National Park Authority  
Responsible Officer: Director of Corporate Services  
Service Manager: Head of Finance and Resources  
Date Issued: 20 March 2013  
Status: Final  
Reference: 56850/004
Summary and Overall Conclusions

Introduction

The SUN accounting system is the overall function that manages the finances of the Authority. It allows journals to be undertaken to move or reallocate the payments and income. From 2010 the Proactis Purchasing System formed a front end to the SUN system for the purchase ledger.

According to the Financial Regulations, the Director of Corporate Services has a statutory responsibility to ensure that adequate systems and procedures are in place to account for all income due and expenditure payments made on behalf of the Authority.

Objectives and Scope of the Audit

The objective of the audit was to provide management with assurance that, in relation to Main Accounting:

- Opening balances were brought forward to the appropriate account and that amounts were correct;
- All debits and credits to the main accounting system netted to zero;
- Data input to the main accounting system was accurate;
- Regular reconciliations were carried out;
- Journal transfers contained adequate explanation and were approved; and
- The system was secure from unauthorised amendment.

In respect to Budgetary Control, that:

- The budget covered all areas of income and expenditure;
- The budget had been fully loaded onto the main accounting system;
- Income and expenditure was monitored;
- Virement limits were set at an appropriate level and were adhered to; and
- The overall budgetary position was monitored promptly and regularly throughout the year, and any significant variances were identified and investigated.

Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided High Assurance.

There were no significant issues raised with management.
Audit Opinions

Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit.

Our overall audit opinion is based on 5 grades of opinion, as set out below.

<table>
<thead>
<tr>
<th>Opinion</th>
<th>Assessment of internal control</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Assurance</td>
<td>Overall, very good management of risk. An effective control environment appears to be in operation.</td>
</tr>
<tr>
<td>Substantial Assurance</td>
<td>Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.</td>
</tr>
<tr>
<td>Moderate assurance</td>
<td>Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.</td>
</tr>
<tr>
<td>Limited Assurance</td>
<td>Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.</td>
</tr>
<tr>
<td>No Assurance</td>
<td>Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.</td>
</tr>
</tbody>
</table>

Priorities for Actions

| Priority 1 | A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management. |
| Priority 2 | A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management. |
| Priority 3 | The system objectives are not exposed to significant risk, but the issue merits attention by management. |
### Annex 2

#### Severity

| Unlikely to have much impact on the integrity of the system or the effectiveness of controls | Over time, is likely to undermine the effectiveness of controls and/or result in reduced efficiency | Issue is so severe that fundamental controls within the system will not operate effectively exposing the system to catastrophic failure. |

#### Probability

| Highly unlikely to occur (timescales will vary with the system being reviewed) | Likely to occur on a regular basis but not frequently (will vary with the system) | Certain to occur in the near future. |
INCOME, CASH AND BANK
YORKSHIRE DALES NATIONAL PARK AUTHORITY
INTERNAL AUDIT REPORT 2012/13

Business Unit: Yorkshire Dales National Park Authority
Responsible Officer: Director of Corporate Services
Service Manager: Head of Finance and Resources
Date Issued: 20 March 2013
Status: Final
Reference: 56565/004

Overall Audit Opinion
Substantial Assurance

Findings

<table>
<thead>
<tr>
<th>P3</th>
<th>P2</th>
<th>P1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Overall Audit Opinion
Substantial Assurance
Summary and Overall Conclusions

Introduction
The authority performs various functions which involve the receipt of income; these include running of the visitor centres, the control of the car parks, and receiving the required payments for planning applications. The authority has established procedures for all these functions.

Objectives and Scope of the Audit

The objectives of the audit were to provide management with assurance that there were adequate controls in place surrounding the receipt, banking and accounting of income from car parks, planning fees and visitor centres.

Testing was restricted to the period from 1st April 2012 to 31st December 2012.

Key Findings

The Authority may be in breach of the Data Protection Act by retaining credit card receipts for longer than is necessary.

Overall Conclusions

It was found that the arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.
Area Reviewed: Data Protection Issue - Retention of Credit Card Information

1. Issue/ Control Weakness | Risk
--- | ---
Personal information is being retained for a period longer than is necessary for payment to be received. | The Authority may be in breach of Data Protection Act by retaining personal information when it is not appropriate to do so.

Findings
When checking the retained credit card receipts at Reeth Visitor Centre it was found that they were retaining the merchant copy with the full details of the purchaser and the card used. It was advised that under the retention policy these are to be retained for six years plus the current year.

The Authority may be in breach of the Data Protection Act by retaining personal information for a period longer than is necessary to secure payment and to consider the risks associated with retaining personal information beyond the period of time that is necessary.

1.1 Agreed Action
Procedures will be put into place to ensure that all the personal information on the merchant copies of the credit card receipts are blacked out after two months. Up until this time they will all be kept in a secure area in the relevant establishment.

Priority | 2
--- | ---
Responsible Officer | Director of Corporate Services
Timescale | 30 June 2013
Overall Audit Opinion: High Assurance
Summary and Overall Conclusions

Introduction
The Yorkshire Dales National Park Authority has its own Human Resources department which plays a key role in the recruitment and selection of staff. The department is also responsible for employee relations, the learning, development and training of staff and health and wellbeing.

In April 2012 the authority brought the payroll function in-house and has since been processing their own payroll. This procedure is managed within the Finance department with additional support provided by Human Resources.

The assignment was a systems based audit and reviewed the systems and controls in place. The authority has established procedures for all these functions.

Objectives and Scope of the Audit
The objective of the audit was through sample testing to provide management with assurance that the controls in place were adequate to ensure that:

- Checks were made in respect to an individual’s right to work in the UK, employee qualifications, medical clearances, references and Criminal Records Bureau (CRB) checks;
- Access to data processing and programmes were restricted to only appropriate personnel;
- Data entered into the payroll system was validated and timesheets were certified;
- Exception reports were generated and reviewed and outputs were checked for reasonableness;
- An establishment list was maintained that was reconciled to the payroll system;
- Separation of duties existed between officers responsible for the preparation of the payroll and the payment of employees;
- BACS payments were appropriately processed and authorised with reconciliations made to the main accounting system;

The audit testing covered the period from 01 April 2012 to 31 December 2012.

Key Findings
The only finding of significance was that copies of employees qualifications were not being retained on file where it was identified in the job specification that qualifications are a necessary requirement.

Overall Conclusions
It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided High Assurance.

Area Reviewed: New starters

<table>
<thead>
<tr>
<th>Severity</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issue/ Control Weakness</td>
</tr>
<tr>
<td>---</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td>Copies of qualifications are not being retained on file.</td>
</tr>
</tbody>
</table>

**Findings**

From the sample of new starters selected testing was undertaken to ensure copies of qualifications were being retained on file where it was identified in the job specification that these particular qualifications were required. For three of the sample selected such copies had not been retained. These were for the Communications Assistant and for two Relief Information Advisors.

<table>
<thead>
<tr>
<th></th>
<th>Agreed Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>The current procedures will be reviewed and if necessary will be amended.</td>
</tr>
</tbody>
</table>

**Priority** | 3  
**Responsible Officer** | Head of HR and Communications  
**Timescale** | 30 June 2013
Summary and Overall Conclusions

Introduction

Purchasing Orders are raised through the Proactis system by employees of the authority. These orders should then be authorised according to the limits within Financial Regulations. When the Invoice is received by the Finance section it is matched to the order, and this then automatically links the payment into the Sun Financial System. A majority of payments are made through the Bacs banking system but some are still made by cheque.

Objectives and Scope of the Audit

The objective of the audit was to provide management with assurance that, in relation to Creditors and Purchasing:

- Invoices were properly certified and authorised for payment;
- The output was checked for reasonableness;
- Manual payments were minimised and subject to review and authorisation;
- Payments were released independently from authorising officers;

Objectives and Scope of the Audit

The objective of the audit was to provide management with assurance that, in relation to Creditors and Purchasing:

- Invoices were properly certified and authorised for payment;
- The output was checked for reasonableness;
- Manual payments were minimised and subject to review and authorisation;
- Payments were released independently from authorising officers;
• Payments were made within targets;
• The creditors system was reconciled;
• The coding of invoices was checked for reasonableness;
• VAT was accounted for and recovered where appropriate; and
• Purchase cards were being used in accordance with YPNPA policies and procedures.

Testing was restricted to the period from 01 April 2012 to 31 December 2012.

Key Findings

It was found that VAT in respect of purchases made was not always reclaimed, particularly when using the purchase card to make purchases from Amazon Market Place, and that one employee had failed to update her declaration of interest to cover her husbands dealings with the authority as a one off supplier.

Overall Conclusions

It was found that the arrangements for managing risk were very good. An effective control environment appears to be in operation. Our overall opinion of the controls within the system at the time of the audit was that they provided **High Assurance**.
Area Reviewed: VAT and retention of receipts

1 | Issue/ Control Weakness | Risk
---|------------------------|--------------------------------------------------
1 | VAT is not being reclaimed for purchases made through the Amazon Market Place. | The VAT claim to HMRC may be understated resulting in a loss of income to the Authority.

Findings

An issue was found when checking the purchases made by procurement cards through the Amazon Market Place.

On 21 May 2012 an order was placed through the Amazon Market Place to the value of £89.99. There was an additional charge of £5.00 for packing and postage. A VAT receipt had not been obtained and therefore the VAT of £15.83 could not be reclaimed. A further order was placed for £20.98. Again there was a copy of the order on file but as no VAT receipt was obtained the VAT of £3.50 could not be reclaimed. The transaction log had been correctly completed by the Volunteer Support Officer in both instances and no VAT was claimed back from HMRC.

A further transaction log dated 31 December 2012 and completed by the Volunteer Support Officer was reviewed. A purchase had been made through the Amazon Market Place at a net cost of £29.94. No VAT receipt had been obtained or reclaimed. A further purchase was made from Sourcing4U Ltd for £210.00 including VAT of £34.99. A VAT invoice was enclosed and the correct amount had been accounted for and claimed.

A similar issue was found when reviewing the transaction log dated 1 July 2012 and completed by the Museum Manager. Again purchases had been made through the Amazon Market Place. Nine items had been purchased with VAT of £4.70 for one of the items being reclaimed from HMRC. There were no VAT receipts on file for any of the nine items purchased.

1.1 | Agreed Action
---|---
The Head of Finance and Resources has emailed everyone in the authority who has a procurement card reminding them that they must get a VAT receipt.

The Head of Finance and resources identified that the other controls in place would limit the amount of exposure to this risk. Those controls are the limit on expenditure applicable to anyone holding a Procurement Card. There is also a transaction limit of £250.00, above this limit and the authority will insist on a full invoice from the supplier.

<table>
<thead>
<tr>
<th>Priority</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer</td>
<td>Head of Finance and Resources</td>
</tr>
<tr>
<td>Timescale</td>
<td>Completed</td>
</tr>
</tbody>
</table>
Area Reviewed: Declaration of Interest

<table>
<thead>
<tr>
<th>2</th>
<th>Issue/ Control Weakness</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>No declaration had been made in the Register of Interests.</td>
<td>Inappropriate payments may be made.</td>
<td></td>
</tr>
</tbody>
</table>

**Findings**

A data matching exercise was undertaken to review those payments made to supplier bank accounts where a member of staff also had the same bank account to have their salary paid into. A supplier payment of £300 had been made to a member of staff where the same account was being used for the payment of their salary. The payment had been made against an invoice addressed to the Yorkshire Dales National Park Authority dated 16 November 2011. The invoice was for storage of materials on Wether Fell. The land was being used to store stone which had to be airlifted for the repair of footpaths across the land. Whilst the invoice and payment are not in dispute there was no declaration by the employee of this payment in the Register of Interests. From information provided, the auditors were satisfied that there was no evidence of the payment being inappropriate.

**2.1 Agreed Action**

The employee concerned has now updated her declaration of interest to cover the point raised within this report.

<table>
<thead>
<tr>
<th>Priority</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Officer</td>
<td>Director of Corporate Services</td>
</tr>
<tr>
<td>Timescale</td>
<td>Completed</td>
</tr>
</tbody>
</table>
Summary and Overall Conclusions

Introduction
YDNPA have three main computer systems; SUN systems, SUN Proactis and Carval these being the financial management system, the purchasing system and the payroll system. They are integral to the business operations of YDNPA to enable the preparation of management accounts and statutory returns, the payment to creditors for goods purchased and the payment of staff salaries. They are audited as any compromise to the integrity of these systems or system failure would pose significant risk to the continued business operations of the Authority.

Objectives and Scope of the Audit
The objective of the audit was to provide assurance that effective controls were in place to address the following key risks:
- The inability to recover and maintain continuity of business following catastrophic failure
- The integrity of key data is compromised
- The loss of physical assets; and
- The links to other key systems fail to operate.
Key Findings
The IT Policy and Procedures were approved in November 2012 however there is concern that it is not intended to undertake a review of these until November 2017. The Risk Register controls make reference to a disaster recovery plan that no longer exists under that name but are incorporated in Annex 5 of the IT Policy and Procedure. This could cause confusion if not clarified. The Authority has good procedures in place for the backing up of data and enforcing password changes.

Overall Conclusions
It was found that the arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.
Area Reviewed: Review of IT Policy and Procedures

<table>
<thead>
<tr>
<th>1</th>
<th>Issue/ Control Weakness</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and procedures may not be reviewed at sufficiently regular intervals.</td>
<td>The IT Policies and Procedures may not keep up to date with the changes in Information Technology if not reviewed in a timely manner putting the Authority at risk of not being compliant with industry expectations.</td>
<td></td>
</tr>
</tbody>
</table>

**Findings**

The authority updated their IT Policies and Procedures in November 2012 and these were subsequently approved by the Senior Management Team. The IT Policies and Procedures are not scheduled to be reviewed again until November 2017.

Consideration should be given to reviewing these policies and procedures earlier because of the pace of change within Information Technology.

**1.1 Agreed Action**

The review period is the default period for the Authority’s Policies and Procedures. The IT Policies would be reviewed in the event of any significant change, such as in legislation, moving to a ‘cloud base’ etc. These Policies will be kept under constant review.

<table>
<thead>
<tr>
<th>Priority</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Responsible Officer</strong></td>
<td>Director of Corporate Services</td>
</tr>
<tr>
<td><strong>Timescale</strong></td>
<td>Completed</td>
</tr>
</tbody>
</table>
### Area Reviewed: Risk 27 of the Risk Management Register

<table>
<thead>
<tr>
<th>#</th>
<th>Issue/Control Weakness</th>
<th>Risk</th>
<th>Severity</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Not all the controls are identified in the Authority's Risk Register.</td>
<td>Management may not be able to manage the risk effectively.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Findings**

The IT related risks in the Authority's Risk Register are identified under risks 27 and 28.

The identified counter measures for Risk 27 - Loss of IT system and records of which the consequences are identified as Severe state, 'Systems capable of independent operation (network resilience); disaster recovery plan'. Consideration should be given to reviewing the terminology used for clarification so that reference is not made to a document that no longer exists under that name. There is an established programme of back ups of the data which are identified in Annex 5 of the IT Policy and Procedures. These are not specifically included within Annex 6 Disaster Recovery Procedures.

**2.1 Agreed Action**

The policies will be amended as soon as possible to correct the above issue.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Responsible Officer</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Head of Finance and Resources</td>
<td>30 June 2013</td>
</tr>
<tr>
<td>Area Reviewed: Access permissions</td>
<td>Severity</td>
<td>Probability</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>Issue/ Control Weakness</td>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Records have not been closed down or set up correctly.</td>
<td>Inappropriate access may be gained.</td>
<td></td>
</tr>
</tbody>
</table>

**Findings**

When a member of staff leaves the Authority their access permissions should be stopped one month after IT have been notified. For the three leavers who have left the Authority this financial year employee 100219 who left on 31 August 2012 should have had their access permissions stopped at the end of September. However, at the time of the audit in January 2013 the account was still live.

3.1 **Agreed Action**

Action will be taken to ensure that the access permissions are removed

<table>
<thead>
<tr>
<th>Priority</th>
<th>Responsible Officer</th>
<th>Timescale</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Director of Corporate Services</td>
<td>Immediate</td>
</tr>
</tbody>
</table>