

## THE BROADS AUTHORITY

### Report of the Head of Internal Audit

#### ANNUAL REPORT ON INTERNAL AUDIT ACTIVITY 2008-09

##### 1. Summary

1.1 The purpose of this report is to satisfy the requirements of the Accounts and Audit Regulations 2003, the Accounts and Audit Regulations (Amendment) (England) 2006 and the Head of Internal Audit's annual reporting requirements set out in the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom 2006. The Code specifies in Section 10.4 that the following information should be forthcoming:

- Include an opinion on the overall adequacy and effectiveness of the organisation's control environment.
- Disclose any qualifications to that opinion, together with the reasons for the qualification.
- Present a summary of the audit work from which the opinion was derived, including reliance placed on work by other assurance bodies.
- Draw attention to any issues the Head of Internal Audit judges particularly relevant to the preparation of the Annual Governance Statement
- Compare the actual work undertaken with the planned work and summarise the performance of the internal audit function against its performance measures and targets.
- Comment on compliance with the Standards of the Code.
- Communicate the results of the internal audit quality assurance programme.

##### 2. Recommendations

It is recommended that the Authority:

- 2.1 Receive and note the Annual Report of the Head of Internal Audit.
- 2.2 Note the overall standards of internal control were **adequate** during 2008/09.
- 2.3 Note that a **limited** assurance has been given in respect of Corporate Governance and Risk Management arrangements for the year ended 31 March 2009.
- 2.4 Note that the adequate opinion provided in respect of the overall standards of internal control and limited assurance opinion in respect of corporate governance and risk management are reflected in the Council's Annual Governance Statement for 2008/09, which is also presented to the Authority.

### **3. Information, issues and opinion**

#### **3.1 Arrangements at the Council for the Provision of the Internal Audit Service**

3.1.1 This is the first full year that the Broads Authority has been part of the Norfolk Internal Audit Consortium, with Audit Management provided by South Norfolk Council and the audits projects appearing on the Annual Audit Plan being performed by Deloitte and Touche Public Sector Internal Audit Ltd.

3.1.2 Although the contractor has experienced slippage when undertaking audits at some participating authorities within the Consortium, this has not impacted significantly on the 2008/09 Annual Audit Plan for the Broads Authority, which was effectively completed in April 2009.

3.1.3 Eight audit reports have been produced for the Authority during 2008/09, which represents a significant increase in the number of audit days and individual audit projects being provided, compared with previous years. Hence, it has been possible to adopt a wider remit that has included a focus on computer audit in terms of carrying out an assessment of disaster recovery arrangements, as well as undertaking a computer audit needs assessment.

3.1.4 The new arrangements have inevitably resulted in a corresponding increase in the cost of Internal Audit for the Authority. Internal Audit fees have totalled £14,693, comprising 2 main elements:

- Cost of Deloitte and Touche auditors: £9,300
- Cost of Audit Management Team input: £5,393

3.1.5 Balancing the requirements of meeting tight job budgets against the need to ensure that audits have the desired level of coverage has remained a problem in year, with the contractor frequently finding it difficult to complete assignments within 3 to 5 day timescales provided in the Annual Audit Plan. Essentially, the contractor has had to produce an audit brief, undertake fieldwork, hold debrief or exit meetings as necessary and prepare audit reports within the days available. Since this has proved difficult to accommodate with reference to the majority of audit projects carried out in 2008/09, the Annual Audit Plan for 2009/10 has been considerably reworked to ensure more realistic job budgets are provided and this had led to a reduction in overall projects to be completed going forward.

#### **3.2 Opinion of the Head of Internal Audit on the Overall Adequacy of the Internal Control Environment at the Broads Authority**

3.2.1 The Opinion contained within this report relates to the system of internal control at the Broads Authority and the overall control environment in place.

3.2.2 The system of internal control is designed to manage risk to a reasonable level rather than to eliminate the risk of failure to achieve corporate/service policies, aims and objectives; it can therefore only provide reasonable and not absolute assurance of effectiveness. The system of internal control essentially relies on an ongoing process designed to identify and prioritise the risks to the achievement of the Broads Authority's policies, aims and objectives, to evaluate the likelihood of those risks being realised and the

impact should they be realised, and to manage them efficiently, effectively and economically.

- 3.2.3 The control environment encompasses the systems of corporate governance, risk management and internal control, hence, the Head of Internal Audit's Annual Opinion seeks to provide an independent assessment of the effectiveness of the control environment, through its reviews linked to the areas of corporate governance and internal control.
- 3.2.4 In reaching an overall opinion, the outcomes of work performed by the Internal Audit Services contractor has been evaluated by the Head of Internal Audit. **Appendix 2b** documents the assurance levels provided in relation to planned audit work that the Deloitte and Touche auditors have carried out at the authority during the year, whilst **Appendix 2a** contains the definitions/categories for the levels of assurance identified.
- 3.2.5 On the basis of internal audit work undertaken in 2008/09, **it is my opinion that the overall standards of internal control are adequate at the Broads Authority for the year ended 31 March 2009** and hence, accord with proper practice. This opinion is derived from separate opinions applying to financial systems and non-financial systems, as detailed in **Appendix 2b**. However, there has also been an occasion, as indicated in **Appendices 1 and 2b**, where limited assurance has been applicable. Limited assurance essentially acknowledges the existence of significant internal control issues which need to be addressed; otherwise their continuing presence would undermine the internal control environment at the authority.

### 3.3 Basis of Assurance

- 3.3.1 All audits have been performed in accordance with the mandatory standards and good practice contained within the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom 2006, the specifications stated in the Internal Audit Services Contract between South Norfolk Council and Deloitte and Touche Public Sector Internal Audit Ltd, plus the standards laid down by Deloitte and Touche's own internal quality assurance systems.
- 3.3.2 **The opinions stated in paragraphs 3.2.5 and 3.6.1 of this report are derived from the work carried out by the Deloitte and Touche auditors over 2008/09 and in the course of the first quarter of 2009/10.** The work performed has been cognisant of the principal risks identified in the Authority's Corporate Risk Register (details of which were used to develop the Annual Audit Plan for 2008/09), and, responsive to changing priorities and additional requirements arising during the year.

### 3.4 Review of the Effectiveness of Internal Audit

- 3.4.1 In order for the Broads Authority to be able to place reliance on the opinions contained within this report, the Head of Internal Audit has in place a performance management and quality assurance framework to demonstrate that the Internal Audit Service is:
- Meeting its aims and objectives;
  - Compliant with the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom 2006;

- Meeting internal quality standards;
- Effective, efficient and continually looking to improve service delivery; and,
- Adding value and assisting the Council in achieving its objectives.

Demonstrable evidence of the framework and the range of information feeding into it, are detailed within this report, and have influenced the agendas for monthly progress meetings with the Section 17 Officer throughout 2008/09. The circulation and receipt of post audit feedback forms, and the completion of an annual exercise to confirm compliance with the Code of Practice (the outcomes of which have been circulated to the Section 17 Officer and have been shared with External Audit to assist their triennial review of Internal Audit in the last quarter of 2008/09) have also played a major part in the evidence gathering process.

3.4.2 Although compliance with the Code of Practice continues to remain at a reasonable level, there are two core areas where full compliance is compromised:

- The Authority has not established an independent Audit Committee that approves Internal Audit's Terms of Reference, Code of Ethics, Strategy, Annual Plans and Annual Report.
- A joint working protocol, alongside formal arrangements for liaison with external audit, is yet to be established. However, to date, External Audit has been given access to final internal audit reports, upon request.

3.4.3 The Head of Internal Audit is currently waiting to discuss preliminary findings arising from External Audit's triennial review of Internal Audit. A meeting is being convened in July 2009 to explore the key outcomes but in the meantime, it is not possible to incorporate the draft findings in the 2008/09 Effectiveness exercise, as these particulars have yet to be properly discussed and formally agreed.

### 3.5 Issues relevant to the Annual Governance Statement

3.5.1 In accordance with Regulation 4 of the Account and Audit Regulations 2003, the Council is responsible "*for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of that body's functions and which includes arrangements for the management of risk*". With effect from 1<sup>st</sup> April 2007, an Annual Governance Statement has to be completed, which focuses on the governance framework at the Council and draws upon many sources of assurance, such as:

- Directors and managers;
- The responsible financial officer;
- The monitoring officer;
- Members;
- The Head of Internal Audit;
- Performance and risk management;
- Third parties, e.g. partnerships; and,
- External audit and other review agencies.

3.5.2 To assist the process outlined in paragraph 3.5.1 above, Internal Audit has recently undertaken work to:

- Assess the current position prior to preparing the Annual Governance Statement, taking into account the findings of internal audit reviews conducted throughout 2008/09.
- Examine the operation of key controls for each of the main financial systems not subject to planned systems audit review in the course of the financial year.
- Revisit the status of high, medium and low priority audit recommendations previously accepted by management in order to gauge the extent to which the internal control environment is being further developed by management to address the risks facing their services.
- Analyse whether the authority has sufficiently robust systems and processes in place for corporate governance, and for the identification and management of strategic and operational risks.

3.5.3 Adequate assurances in respect of the Authority's core financial systems have been gained from the following audits:

- BA/09/03 Toll Income (Income Receivable)
- BA/09/04 Asset Management (Fixed Assets)
- BA/09/05 Payroll and HR (Payroll and Pensions)
- BA/09/07 Key Controls (General Ledger maintenance, Budgetary Control, Fixed Assets, Cash and Treasury Management, Purchasing and Payables / Creditors, Income Receivable / Debtors)

Management Summaries in respect of these audits can be found at **Appendix 3** to the report.

3.5.4 In addition to those audit reports finalised in year, it is important to note that 4 audits were not fully completed until after 31 March 2009 and that these particular reviews generated 4 high priority recommendations as follows:

- BA/09/02 – Computer Audit Needs Assessment – 1 high priority recommendation has been reported to management (a copy of the full report is attached at **Appendix 4**)
- BA/09/04 – Asset Management – 1 high priority recommendation has been agreed with management
- BA/09/06 – Disaster Recovery – 2 high priority recommendations have been agreed with management, and overall, a limited assurance was found to be applicable to operational arrangements in this area.

The high priority recommendations are identified in the Management Summaries for these audits included at **Appendix 3** and in the Computer Audit Needs Assessment Report at **Appendix 4**; although they are not due for implementation until after 31 March 2009, they should be noted in the Annual Governance Statement for 2008/09.

3.5.5 In terms of management's response to the implementation of agreed audit recommendations, **Appendix 5** provides an overview of the current status of those recommendations. There have been 19 recommendations raised in year, which required implementation by 31 March 2009, of which 4 (1 medium priority, 3 low priority) are still outstanding. A further 26 recommendations are due for implementation after 31 March 2009 and as

already mentioned in paragraph 3.5.4 above, 4 of these have high priority ratings.

3.6 Opinion of the Head of Internal Audit on the Overall Adequacy of Corporate Governance Arrangements and Risk Management at the Broads Authority

3.6.1 On the basis of Internal Audit work undertaken in respect of Corporate Governance and Risk Management arrangements for 2008/09, **it is my opinion that a limited assurance level can be given to the corporate governance framework and risk management arrangements within the Authority for 2008/09.** This level of assurance was obtained following the completion of Audit Ref. No. BA/10/01, for which a draft report has been produced and is currently subject to discussion with management. This piece of work actually forms part of the 2009/10 Annual Audit Plan for the Broads Authority but has looked back over arrangements in place for 2008/09.

**4. Audit work undertaken in respect of 2008/09**

4.1 Delegated authority was given by the Broads Authority meeting of 28 March 2008 to the Director of Corporate Services, Head of Finance, and the Head of IT and Collector of Tolls to collectively approve the 2008/09 Annual Audit Plan. Following agreement of the Plan, an additional 3 days of audit work was requested to evaluate the Annual Governance Statement for 2007/08, and an additional day of work was allocated to facilitate further key control testing. The other notable variation to days delivered is the increase in audit management input for 2008/09, which was substantially underestimated when the Annual Audit Plan was originally developed.

4.2 The table below shows in summary the audit coverage that was planned compared with what has actually been delivered, whilst a more detailed overview is attached at **Appendix 1** to the report, detailing when the individual audit assignments were completed and total audit management input provided. Reference is also made to the ad-hoc work that was undertaken in year.

Description	Days planned for 2008/09	Days delivered	% of planned days delivered
Systems audit	24	33.4	100%
Computer audit	8	8	100%
<b>Total</b>	<b>32</b>	<b>41.4</b>	<b>100%</b>
Extra Work requested		3	

4.3 The annual audit plan for 2008/09 was completed on 23 April 2009.

**5. Performance of the Audit Service 2008/09**

5.1 In addition to ensuring delivery of specific work in the Annual Audit Plan, the Internal Audit Services contract provides for the service to be measured against the following indicators, as tabulated overleaf.

Description of indicator	Target	Achievement of Deloitte and Touche auditors – April 2008 to April 2009
Average time taken to issue draft audit reports following the completion of audit fieldwork	10 working days	21.3
Average time taken to convert draft reports into final audit reports	15 working days	26.7
Average time taken between the completion of audit fieldwork and the issue of final audit reports	25 working days	48.0
Percentage of audit recommendations accepted	90%	100%

5.2 As can be clearly seen above, the time between the completion of the audit fieldwork and the production of final audit reports is not in line with contract requirements and needs to improve. With this in mind, the contractor, Deloitte and Touche, has been working to identify ways in which to ensure that reports are produced on a timelier basis in the future. It is hoped that the introduction of debrief meetings when fieldwork is nearing completion will resolve issues ahead of draft reports being produced, and thus help to bring down the timeframes involved in extracting draft and final reports subsequently.

5.3 It is pleasing to note that management has accepted all of the recommendations raised in year.

5.4 To assist the audit work going forward, the contractor's Engagement Manager and Field Manager held a planning meeting with the Director of Corporate Services in May 2009 to agree the dates for all audits within the 2009/10 audit plan, and identify the key contacts for each audit. In this regard, it is hoped that the audit plan should be progressed more smoothly.

## 6. Review of High Priority Recommendations

6.1 It is important to ensure that audit recommendations, which have been accepted by officers, are then implemented within the deadline dates agreed, if the internal control environment is to improve. All high priority recommendations raised in year are due to be implemented after 31 March 2009.

## 7. Recommendations

7.1 To receive and note the contents of this report in relation to Internal Audit activity and performance in 2008/09, and, the opinions expressed therein.

7.2 To ensure that the opinions given in this report are acknowledged in the Broads Authority's Annual Governance Statement for 2008/09.

## **8. Reasons for Recommendation**

- 8.1 The Broads Authority needs to be aware of Internal Audit's independent assessment of the effectiveness of the organisation's internal control environment (encompassing corporate governance arrangements and systems of internal control) prior to receiving the organisation's Annual Governance Statement for 2008/09.

### Lead Contact Officer:

Name/Post: Mrs. Sandra C. King, Head of Internal Audit, South Norfolk Council

Telephone: 01508 533863

Email: scking@s-norfolk.gov.uk

### Appendices attached to this report:

**Appendix 1:** Review Work delivered in accordance with the Annual Audit Plan for 2008/09 plus Ad-Hoc Work requested by Management

**Appendix 2a:** Definitions/Categories of Audit Opinions relating to Individual Audit Assignments

**Appendix 2b:** Analysis of Assurances in relation to System of Internal Control based on outcomes of Internal Audit Assignments conducted in 2008/09

**Appendix 3:** Abridged Management Summaries relating to Reviews completed by Deloitte and Touche Public Sector Internal Audit Ltd

**Appendix 4:** Final Audit Report in respect of BA/09/02 Computer Audit Needs Assessment

**Appendix 5:** Follow up of Internal Audit recommendations at 31 March 2009

## Appendix 1

**Review Work delivered in accordance with the Annual Audit Plan for 2008/09 plus Ad-Hoc Work requested by Management**

Audit No.	Description of Audit	Frequency of Audit Coverage	Days Planned	Days Delivered	Original Scheduling	Status	Assurance Level applicable	Summary report details presented to the Authority
<b>PLANNED SYSTEMS AUDIT WORK</b>								
BA/09/01	Corporate Governance - Part 1	Annually	3	3	Quarter 1 April 2008	Completed. Final Report issued 03/07/08	Substantial	Jun-09
BA/09/03	Toll Income	2-yearly	3	3	Quarter 2 September 2008	Completed. Final Report issued 23/01/09	Adequate	Jun-09
BA/09/04	Asset Management	2-yearly	3	3	Quarter 3 October 2008	Completed. Final Report issued 07/04/09	Adequate	Jun-09
BA/09/05	Payroll/Human Resources	2-yearly	5	5	Quarter 3 November 2008	Completed. Final Report issued 02/03/09	Adequate	Jun-09
BA/09/07	Key Controls and Assurance work	Annually	5	5	Quarter 4 March 2009	Completed. Final Report issued 17/04/09	Adequate	Jun-09
	Audit Management Team Input	Annual	4	13.4				
	Follow up of previous Systems Audit recommendations	Annual	1	1				
<b>TOTAL PLANNED SYSTEMS AUDIT WORK</b>			<b>24</b>	<b>33.4</b>				

Audit No.	Description of Audit	Frequency of Audit Coverage	Days Planned	Days Delivered	Original Scheduling	Status	Assurance Level applicable	Summary report details presented to the Authority
-----------	----------------------	-----------------------------	--------------	----------------	---------------------	--------	----------------------------	---

**PLANNED COMPUTER AUDIT WORK**

BA/09/02	IT overview/ Computer Audit Needs Assessment	3-yearly	3	3	Quarter 1 June 2008	Completed. Final report issued 23/04/09	n/a	Jun-09
BA/09/06	Disaster recovery - deferred from 2007/08	2-yearly	5	5	Quarter 4 January 2009	Completed. Final Report issued 15/04/09	Limited	Jun-09
<b>TOTAL PLANNED COMPUTER AUDIT WORK</b>			<b>8</b>	<b>8</b>				

<b>TOTAL PLANNED SYSTEMS &amp; COMPUTER AUDIT WORK</b>			<b>32</b>	<b>41.4</b>				
--	--	--	-----------	-------------	--	--	--	--

**AD HOC WORK REQUESTED**

BA/09/01	Work to support preparation of the Annual Governance Statement for 2007/08 - Part 2	At the request of the client	3	3	Quarter 1 April 2008	Completed. Final Report issued 22/09/08	Substantial	Jun-09
----------	---	------------------------------	---	---	-------------------------	--	-------------	--------

<b>GRAND WORK TOTAL</b>			<b>35</b>	<b>44.4</b>				
-------------------------	--	--	-----------	-------------	--	--	--	--

**Definitions / Categories of Audit Opinions relating to Individual Audit Assignments**

Deloitte and Touche Public Sector Audit Ltd have four categories by which they classify internal audit assurance over the processes examined, and these are defined as follows:

<p><b>Good Assurance</b></p>	<p>There is a sound system of internal control designed to achieve the client's objectives.</p> <p>The control processes tested are being consistently applied.</p>
<p><b>Adequate Assurance</b></p>	<p>While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.</p> <p>There is evidence that the level of non-compliance with some of the control processes may put some of the client's objectives at risk.</p>
<p><b>Limited Assurance</b></p>	<p>Weaknesses in the system of internal controls are such as to put the client's objectives at risk.</p> <p>The level of non-compliance puts the client's objectives at risk.</p>
<p><b>Unsatisfactory Assurance</b></p>	<p>Control processes are generally weak leaving the processes/systems open to significant error or abuse.</p> <p>Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.</p>

The assurance gradings provided above are not comparable with the International Standard on Assurance Engagements (ISAE 3000) issued by the International Audit and Assurance Standards Board and as such the grading of 'Good Assurance' does not imply that there are no risks to the stated objectives.

**Analysis of Assurances in relation to System of Internal Control based on  
outcomes of Internal Audit Assignments**

**Audits conducted in 2008/09****Financial Systems**

Description of Audit	Level of Assurance obtained			
	Good	Adequate	Limited	Unsatisfactory
Toll Income		✓		
Payroll and Human Resources		✓		
Asset Management		✓		
Key Controls and Assurance work		✓		

**Non-Financial Systems**

Description of Audit	Level of Assurance obtained			
	Good	Adequate	Limited	Unsatisfactory
Disaster Recovery			✓	

**Audits where no opinion has been given:**  
**Computer Audit Needs Assessment**

**Audits undertaken in relation to the 2007/08 financial year**

Two audits – Corporate Governance, and Work to support the Annual Governance Statement, were undertaken in 2008/09 which related to 2007/08. These have not been considered when producing the audit opinion in respect of 2008/09.

**Audits conducted in 2009/10**

The following audit was undertaken as part of the 2009/10 Annual Audit Plan in respect of the 2008/09 financial year:

**Non-Financial Systems**

Description of Audit	Level of Assurance obtained			
	Good	Adequate	Limited	Unsatisfactory
Corporate Governance and Risk Management			✓	

**Report No. BA/09/03 – Final Report issued 23 January 2009**

**Audit Report on Toll Income**

**Audit Opinion**

Adequate Assurance given

**Rationale to support award of opinion**

The audit work carried out by Internal Audit indicated that:

- While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.
- There is evidence that the level of non-compliance with some of the control processes may put some of the client's objectives at risk.
- The opinion derives from the level of recommendations raised, which relate to the implementation of procedure guidance for staff and utilising the HARPS database.
- The opinion has improved since the last audit visit.

**Summary of Findings**

**Policies and Procedures**

While key staff operating the system are well practised in administrating the system, there is a lack of policy and procedures governing this area. Whilst this is understood to have been a result of waiting for the new computer system that was due to go live in September 2008 and has now been postponed until the new year, there are no existing/previous policy and procedures held.

**Funding and Financial Controls**

Controls are in place for budget setting and monitoring, together with actions to ensure all income due is collected.

Weaknesses in control were identified in effectively using the HARPS and Tolls DMS systems for monitoring of outstanding tolls and the display of registrations, although other manual records were held. Delays in utilising this system to its full potential have been affected by the resource required to implement the new boat safety requirements.

**Performance Information**

The performance targets set by the Authority in relation to toll income are for achieving expected income levels by key dates within the year. The actual income as at September 2008 was overall higher than stated in the budget, resulting in a surplus. This is monitored by the Head of IT and Collector of Tolls and reported monthly to the Director of Corporate Services, Director of Waterways and Navigation Committee. This is detailed in Funding and Financial Controls above.

**Risk Management**

The risk register identifies risks in relation to the Tourism Industry that have an impact on toll income for the Authority and the Authority has recorded measures to address these risks.

The following recommendations have been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	Medium	Low
	Policies and Procedures	<b>Amber</b>	<b>Green</b>	0	1	0
	Funding and Financial Management	<b>Green</b>	<b>Amber</b>	0	1	0
	Performance Management	<b>Green</b>	<b>Green</b>	0	0	0
	Risk Management	<b>Green</b>	<b>Green</b>	0	0	0
<b>Total</b>				<b>0</b>	<b>2</b>	<b>0</b>

#### High Priority Recommendations

No high priority recommendations have been raised as a result of this audit.

Management have accepted all recommendations put forward.

**Report No. BA/09/04 – Final Report issued 7 April 2009**

**Audit Report on Asset Management**

**Audit Opinion**

Adequate Assurance given

**Rationale to support award of opinion**

The audit work carried out by Internal Audit indicated that:

- While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.
- There is evidence that the level of non-compliance with some of the control processes may put some of the client's objectives at risk.
- We have made recommendations based upon concerns regarding the lack of formal procedures for acquisitions and disposals of assets, including the absence an authorisation form.

**Summary of Findings**

**Asset Management**

Controls were found to be in place in respect of ensuring the fixed asset register was kept up to date with accurate values and had adequate insurance cover.

Weakness were found in the absence of an asset management strategy and policies and procedures for asset management, budget monitoring for maintenance expenditure, approval of operating lease expenditure and the lack of regular reconciliations of the fixed asset registers to other records.

**Performance Management**

Controls were found to be in place for setting, monitoring and reporting performance against targets to management.

**Risk Management**

There are controls in existence for the management of risk.

The following recommendations have been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	Medium	Low
	Asset Management	<b>Amber</b>	<b>Amber</b>	1	4	1
	Performance Management	<b>Green</b>	<b>Green</b>	0	0	0
	Risk Management	<b>Green</b>	<b>Green</b>	0	0	0
<b>Total</b>				<b>1</b>	<b>4</b>	<b>1</b>

### High Priority Recommendations

One high priority recommendation has been raised:

#### Asset Management

Policies and procedures should be devised and updated for asset management. These should include procedures for acquisitions and disposals, the authorisation of assets and establishing formal legal agreements for all assets the Broads Authority is responsible for.

Management have agreed all recommendations put forward.

**Report No. BA/09/05 – Final Report issued 2 March 2009**

**Audit Report on Payroll and Human Resources**

**Audit Opinion**

Adequate Assurance given

**Rationale to support award of opinion**

The audit work carried out by Internal Audit indicated that:

- While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.
- There is evidence that the level of non-compliance with some of the control processes may put some of the client's objectives at risk.

**Summary of Findings**

**Policies, Procedures and Legislative requirements**

Controls were found to be in place relating to policies and procedures that were available to staff via the HR section of the intranet. Weaknesses were noted in that the Scheme of Local Conditions had not been updated since 2004.

**Starters and Leavers**

Controls were found to be in place to ensure that starters were appropriately authorised and set up on the payroll system in a timely manner and that documentation to support this was retained. Controls were also in place to ensure that leavers were removed from the payroll system in a timely manner and that documentation to support this was retained. In addition, the Authority has undertaken a reconciliation between payroll data and HR data.

**Deductions and Changes to Payroll Records**

Controls were found to be in place to ensure that all deductions were authorised prior to the deduction being actioned and a month end review of deductions is undertaken.

**Payments and Financial Records**

Controls were found to be in place relating to the recording of all payments. This is monitored and documentation retained by the payroll coordinator at Broadland District Council. Weaknesses were noted in the recording of payments in the accounts, as salary control account reconciliations were not evidenced as completed or reviewed.

**IT Systems and Backups and Contingency Planning**

The payroll function is outsourced and, as such, back up and contingency planning is the responsibility of the payroll service provider, Fujitsu. Controls were found to be in place relating to access to the HR system. However, the Electronic Communications Policy was found to be in need of review to reflect current working practices.

**Human Resources**

Controls were found to be in place to ensure all recruitment was authorised prior to advertisement. Policies and procedures relating to HR were found to be in place and appropriate checks were undertaken on new starters with documentation retained. Weaknesses were found in the annual individual review process, and the Unsatisfactory Work Performance and Related Matters procedure had not been updated since 2004.

### Performance Information

Controls were found to be in place to ensure that performance targets are set in accordance with national HR targets, e.g. number of days absence due to sickness. However, performance against these targets had not been measured in the previous year due to staff absence.

### Risk Management

Controls were found to be in place to ensure that issues arising from Payroll and Human Resource can be escalated from an operational to a strategic level. A full risk register in place for the Broads Authority and this includes risks relating to human resources.

Controls were also found to be in place to ensure that mitigation plans exist and are monitored to prevent strategic risks from being realised.

The following recommendations have been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	Medium	Low
	Policies, Procedures and Legislative Requirements	Green	Amber	0	1	0
	Starters and Leavers	Green	Green	0	0	0
	Deductions and Changes to Payroll Records	Green	Green	0	0	0
	Payments and Financial Records	Green	Amber	0	1	0
	IT Systems Back Up and Contingency Planning	Green	Amber	0	1	0
	Human Resources	Green	Amber	0	2	0
	Performance Information	Green	Amber	0	1	0
	Risk Management	Green	Green	0	0	0
<b>Total</b>				<b>0</b>	<b>6</b>	<b>0</b>

### High Priority Recommendations

No high priority recommendations have been raised as a result of this audit.

Management have accepted all recommendations put forward.

**Report No. BA/09/06 – Final Report issued 15 April 2009**

**Audit Report on Disaster Recovery**

**Audit Opinion**

Limited Assurance given

**Rationale to support award of opinion**

The audit work carried out by Internal Audit indicated that:

- | ⊕ Weaknesses in the system of internal controls are such as to put the client's objectives at risk.
- | ⊕ The level of non-compliance puts the client's objectives at risk.
  - There are a total of two high and one medium priority recommendations that have been raised as there is no documented Disaster recovery (DR) plan in place, and no documented Business Continuity Plan (BCP) for the DR plan to provide guidance to ICT to develop the required Disaster recovery solutions. However, as it has recently been demonstrated that the systems can be re-built from backups through the recent office move, we have been able to provide a limited level of assurance.

**Summary of Findings**

**Critical Business Functions**

The development of a documented BCP is planned in the Governance Statement to be completed by the end of 2009, but currently the Authority has completed limited planning in this area. The BCP should be developed to identify the key services provided by the Authority and this should be used to provide guidance to ICT for the development of disaster recovery arrangements to support the recovery of business processes. Aligning the DR Plan with the BCP helps to identify the critical systems, people and locations required for recovery. Absence of a documented BCP, including recovery priorities would limit the effectiveness of a DR plan developed independently by IT.

Internally within IT there is an awareness of the systems required to be recovered and their recovery order due to the knowledge of the services supported, however, this is not documented and cannot be confirmed as meeting the requirements of the Authority.

**Disaster Risk Assessment**

A risk assessment has not been undertaken to determine the potential threats to the Authority and its key products and services; this in turn would drive the recovery objectives and BCP and DR requirements. There is a Strategic Risk Register in place but this is not in sufficient detail to develop an effective BCP. The risk assessment should be performed at a business level to identify key threats to the organisation. This should then be linked to identify risks pertaining to ICT as there are a number of factors which may impact on people, e.g. avian flu outbreak, but as a result could also impact on IT provision, e.g. extended remote working, which may not be picked up from a purely IT driven analysis.

**Disaster Escalation Procedures**

Disaster escalation decision making, through to invocation of the BCP and DR plan would be the responsibility of the Management team, led by the Chief Executive Officer (CEO) and directors of services (Planning, Waterways, Conservation and Countryside and Corporate

Services), however this process is not fully documented and does not identify the responsibility for invoking the BCP.

### Testing of the Disaster Recovery Plan

There is no documented DR plan or procedures in place within the Broads Authority to aid in the recovery of their IT systems in the event of disaster. There is also a reliance on key members of staff for the recovery of systems, therefore it is imperative that the requirements of the Authority, and the recovery process are clearly documented. The Authority did, however, go through a recent office move which required core applications (excluding Planning) to be migrated to new servers, which was achieved through a backup/recovery process, however these processes were not documented for future reference.

The following recommendations have been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	Medium	Low
	Critical Business Functions / Disaster Risk Assessment / Disaster Escalation Procedures	Red	N/A	1	0	0
	Disaster Escalation Procedures/ Disaster Recovery Procedures	Red	N/A	1	0	0
	Testing of the DR Plan	Red	N/A	0	1	0
<b>Total</b>				<b>2</b>	<b>1</b>	<b>0</b>

### High Priority Recommendations

Two high priority recommendations have been raised, these are in relation to:

- ⊕ Developing and testing an Authority BCP; and
- Developing a DR Plan.

Management have agreed the recommendations put forward.

**Report No. BA/09/07 – Final Report issued 17 April 2009**

**Audit Report on Key Controls**

**Audit Opinion**

Adequate Assurance given

**Rationale to support opinion**

The audit work carried out by Internal Audit indicated that:

- While there is a basically sound system of internal control, there are weaknesses, which put some of the client's objectives at risk.
- There is evidence that the level of non-compliance with some of the control processes may put some of the client's objectives at risk.
  
- This system has previously been audited, and in comparison with previous findings, the level of assurance within our audit opinion is unchanged.

**Summary of Findings**

**Treasury Management / Investments**

Bank balance reports were produced weekly that detail investments, although we noted that for the period of 21/08/2008 - 11/12/2008 no reports had been produced; furthermore, reports that had been produced were not subject to independent review and as such a recommendation is raised. Broadland District Council is responsible for the Authority's investments, providing the Authority with six monthly returns. Due to the nature of payments, a detailed annual report is provided to the Authority by Broadland Council and as such, monthly reconciliations to the general ledger would be impractical. We were made aware of an agreement between the Authority and its fund manager (Broadland District Council) to share any loss incurred as a result of investments, however this had not been formally documented and approved by members.

We also noted that the Authority's Investment Policy was subject to annual review.

**General Ledger**

Sound controls were found to be in place over the automatic carry forward of balances. Furthermore, journals are entered if they balance and those entered are recorded with documentation to support the entries. A recommendation was raised in relation to independent authorisation of journals as an improvement to existing control. Controls were also found to be in place for weekly reconciliations between the Authority's Tourist Information Centres and Boat Stations. We noted that bank reconciliations to the general ledger were taking place, however it was unclear if these were reviewed in a timely manner therefore a priority recommendation has been raised.

Monthly reconciliations of the sales ledger to the general ledger were documented as taking place although due to staff changes, these had not been produced on a monthly basis, and therefore a medium priority recommendation was raised.

Testing identified that the monthly reconciliation of the purchase ledger to general ledger for October 2008 could not be identified. Evidence of agreement of the purchase ledger

reconciliation to the general ledger has not been retained, and could not be obtained retrospectively, due to the Dimensions system not allowing staff to go back to a certain date to validate the reconciliation. A recommendation was raised to retain supporting documentation.

### **Budgetary Control**

We noted that budgets are set in line with an agreed timetable and finalised budgets are communicated to budget holders via the annual budget document. Budgets are entered onto the general ledger and profiled by the budget holder. Budget reports are produced and communicated on a monthly basis via the staff intranet, variances over £10,000 must be explained in the bi-monthly Broads Authority meetings, we did however note some delays in the timeliness of reports and subsequently a delay in going to members. Due to the long term absence of the Head of Finance, we were unable to establish how responsibilities are communicated to budget holders.

### **Creditors / Purchase Ledger**

Invoices require two signatures for authorisation and these are checked to an authorised signatories list. All payments are made through the Authority's DMS on a weekly basis. Suggested payment reports are held on file with the weekly reconciliations and we noted inconsistencies regarding the signing of each of the documents and therefore raised a recommendation.

Controls were found to be in place to ensure batch totals agreed to the manual list before posting and that current batch listing is agreed independently to actual invoices with this being evidenced on the batch header. We were informed that budget holders are required at year end to provide a list of accruals via an email from the Head of Finance but due to her absence we were unable to obtain evidence of this process.

### **Debtors / Sales Ledger**

Controls were found to ensure batch reports are agreed to the ledger as part of the debtors reconciliation. Batch reports are included as part of the monthly debtors reconciliation procedure. We were informed that customers with invoices over 30 days old are sent reminder letters and are identified through the aged debtor reports produced as part of the debtors reconciliations to the general ledger. A recommendation has already been identified to the timeliness of these.

The following recommendations have been raised:

<b>Adequacy and Effectiveness Assessments</b>	<b>Area of Scope</b>	<b>Adequacy of Controls</b>	<b>Effectiveness of Controls</b>	<b>Recommendations Raised</b>		
				<b>High</b>	<b>Medium</b>	<b>Low</b>
	Treasury Management	<b>Green</b>	<b>Amber</b>	0	2	0
	Main Accounting System/General Ledger	<b>Green</b>	<b>Amber</b>	0	2	2
	Budgetary Control	<b>Green</b>	<b>Amber</b>	0	0	1
	Creditors/Purchase Ledger	<b>Green</b>	<b>Amber</b>	0	1	0
	Debtors/Sales Ledger	<b>Green</b>	<b>Amber*</b>	0	0	0
<b>Total</b>				<b>0</b>	<b>5</b>	<b>3</b>

\* Recommendations raised in Main Accounting System/General Ledger also apply to the Debtors/Sales Ledger area of the audit hence the status of Effectiveness of Controls being Amber, despite no recommendations being raised.

**High Priority Recommendations**

No high priority recommendations have been raised as a result of this audit

Management have agreed all recommendations put forward.

**Appendix 4**

**BA/09/02 COMPUTER AUDIT NEEDS ASSESSMENT**

**Broads Authority**

**April 2009**

## **CONTENTS**

<b>SECTION</b>	<b>PAGE</b>
<b>1. INTRODUCTION</b>	<b>1</b>
<b>2. AUDITABLE AREAS</b>	<b>1</b>
<b>3. RISK ASSESSMENT APPROACH</b>	<b>2</b>
<b>4. BROADS AUTHORITY BACKGROUND</b>	<b>2</b>
<b>5. IT SUPPORT AT THE BROADS AUTHORITY</b>	<b>3</b>
<b>6. POTENTIAL AREAS OF COVERAGE</b>	<b>4</b>
<b>7. AUDIT COVERAGE IMPLICATIONS FOR THE ANNUAL AUDIT PLAN FOR 2009/10 AND THE STRATEGIC AUDIT PLAN FOR 2009/10 TO 2013/14</b>	<b>6</b>

---

## 1. INTRODUCTION

We are pleased to present our Computer Audit Needs Assessment and Strategic Plan for the Broads Authority. We believe that such an assessment is a vital component of the planning process and allows direction of audit effort towards areas of risk within the IT environment that are of specific importance to the Authority. Our approach reflects our philosophy that the computer audit function should be seen as a constructive management tool that provides useful advice to management on the efficiency and effectiveness of systems, procedures and operations. This approach has been successfully introduced across a wide range of our clients with annual Audit budgets of less than twenty days per annum, including those in the Public Sector.

The following sections give further details of how our assessment has been conducted and the conclusions we have reached.

## 2. AUDITABLE AREAS

We assess the risk areas in terms of a number of audit areas so that audit types are distinguished by different audit risk objectives, e.g. Network Reviews, Security and Control Reviews, System Reviews and Management Controls.

The nature of auditable areas differs between audit types, e.g. for a system review the auditable area can be within a specific installation, for a controls review it can be Authority wide, departmental, outsourced, or some combination of these, and impact on a variety of corporate risks. These areas are discussed during interviews to establish the key risk areas within the authority.

It is important to note that although audits are planned separately, so that the appropriate criteria can be applied to each type of audit, it may be appropriate to combine audits for the purposes of execution. Where this is in the best interest of the Authority, synergy between audits has been sought in the development of each audit scope set out in section 6.

The following notes set out the ground rules and the proposed definitions of units for each of the audit types.

### Ground rules

As far as practicable, the audit types have been divided so that the auditable areas:

- are comparable with each other - significance analysis is ineffective if unlike units are compared, e.g. comparing an existing system with a project;
- represent logical groupings which will result in an efficient use of audit resources;
- reflect the reporting lines within the organisation so that any issues raised have immediate relevance to an identified management team and the channels for communicating findings are clear;
- provide a reasonably homogeneous population, especially as regards size - there should not be extremely large or extremely small audit units in the same population; and
- are of manageable size.

---

### **3. RISK ASSESSMENT APPROACH**

#### **Auditable areas**

In order to identify the auditable areas and establish the areas of risk or specific importance within the Authority, we adopted an approach involving discussion and review of the current position, a review of the current risk register, and a visit to the Authority's primary site, DragonFly House. Information was gathered by undertaking an initial interview with the Head of IT and Collector Of Tolls. These discussions, along with the Authority risk register have formed the basis for this needs assessment.

Auditable areas have been classified into three bands according to their perceived significance. These bands have been used to determine the priority of audits to be undertaken. Band High (H) is the highest and contains the systems identified as of most significance to the organisation.

Those in the higher bands will normally be audited more frequently and to greater depth than those in the lower bands, unless special requirements arise as a result of specific management concerns about an area.

### **4. BROADS AUTHORITY BACKGROUND**

The Broads Authority was set up in 1989 as a statutory body with a general duty to manage the Broads for the purposes of:

- conserving and enhancing the natural beauty, wildlife and cultural heritage of the Broads;
- promoting opportunities for the understanding and enjoyment of the special qualities of the Broads by the public; and
- protecting the interests of navigation.

The Broads Authority runs on a committee structure and the members who sit on the Authority are appointed from local Councils and by the Secretary for the State and environment.

The Broads Priorities 2006/07 - 2008/09 can be found on their website and include (Amongst others):

- Implement an integrated approach to the management of land and water.
- Deliver an excellent planning service.
- Guide the activities of the boating community and local organisations to provide a safe environment for navigation using the Safety Management System.
- Reach a wider audience with appropriately interpreted information and opportunities for enjoying the special qualities of The Broads.
- Increase the organisational and financial capacity of the Authority and minimise its carbon footprint.

In order to help the Authority achieve these it is imperative that the IT Infrastructure which supports these Priorities is appropriately managed and geared to the tasks in hand.

---

## 5. IT SUPPORT AT THE BROADS AUTHORITY

### User Base:

At peak times the IT systems support up to 150 users, which include permanent and seasonal staff in services such as information centres. Of These there are approximately 120 Permanent employees across three sites and working from remote locations, including:

- Approximately 75 Core users based in DragonFly House;
- 12 users based in the Ludham offices; and
- 6 users based in dockyard operations; and
- 4 users at Beccles.

These remote sites are connected via Virtual Private Networks (VPN) with Domain controllers at DragonFly house, Ludham and Beckles.

### Applications:

**There are a number of IT applications used at the Authority, of which the key ones are used for:**

- Planning applications and records - (IDOX Uni-Form);
- Vessel Registrations – including licensing - (HARPS HARbour and Ports System);
- Finance system - (Access Dimensions);
- GIS – ESRI Product;
- CAMS – Countryside Access Management Systems - (Exegesis CAMS);
- NAMS – Navigational Access Management Systems - (Exegesis CAMS);
- HR System – (Snowdrop);
- Document Management – (Sharepoint)

### DragonFly House:

DragonFly house is a new building within the City of Norwich. The facility is owned and managed by DEFRA and houses five companies on various floors of the Building. The Broads Authority office space is open plan and there are no access controls in place to prevent other

---

organisation personnel entering the Authorities office areas. This is an area of concern for Audit as this leaves any equipment in the office area vulnerable to unauthorised access, including laptops, desktops and paperwork left overnight or at weekends. Audit would recommend that the offices are appropriately secured against unauthorised access (Appendix 2).

**Remote Access:**

There are three levels of remote access used within the Authority, all managed via VPN. This allows users to connect their laptops to the Authority's network from remote locations, allows a small number of TREO phones to be synchronised, and allows IT Service support services to connect in to support IT systems. There are also currently around 40+ laptops in use on and off site across the Authority.

**Operating systems:**

The Broads Authority run predominantly on a Microsoft Windows based environment and consistency is sought across the infrastructure as follows:

- The main server Operating System (O/S) is Windows 2003;
- The main Laptop and Desktop O/S is Windows XP;
- Sharepoint is Microsoft Sharepoint 2003, however the Authority wants to move to Microsoft Office Sharepoint Server (MOSS) 2007; and
- Desktop office applications use Microsoft Office 2007.

**Server room and Backups:**

The main building is managed by Defra, and the Authority has access to a shared server room to manage their own systems which should be held in key and combination locked cabinets, however at the time of the needs assessment the combination locks did not work. Broads Authority staff have access to the server room for management of backup tapes. Audit would recommend that the Cabinet locks are fixed as a matter of urgency (Appendix 2).

**6. POTENTIAL AREAS OF COVERAGE**

Due to the time allocation for Computer Audit we are not able to offer a full three year plan, rather we have identified the key areas within the needs assessment and put together a shortlist of relevant audits for the Authority to discuss internally and decide on the most appropriate course of action. This could include the Authority undertaking a self assessment against best practice guidelines or having the audit carried out. To aid in the selection process a \* rating has been applied to each audit with \*\*\* covering what are believed to be the highest risk areas, based on the authorities profile, and \* being the lowest. Further discussions should be undertaken internally in order for the Authority to determine their risk appetite within each of these areas before a final decision on coverage and approach is made. Where possible we have consolidated work to give synergy between areas to provide best value. Where necessary these can be split out into smaller segments of work, however undertaken individually will require more Audit time.

---

Based on the risk profile of IT Auditable areas (Appendix 1) the following areas have been highlighted as potential areas for Audit:

**1) IT Governance, Strategy and Policy\*\*\* – 9 Days**

The authority has grown quickly since it was first formed in 1989 and is now at a stage where more formal communication lines, not only within IT but between IT and the rest of the Authority Departments, are required in order to effectively manage the IT Environment. An Audit of the Governance structure would provide the Authority with assurance that this structure is in place so that IT are in a position to help the Authority achieve their priorities. IT Strategy will help ensure that IT delivery priorities are aligned with the Authority's medium and long term visions, and IT Policy will provide a framework for the management and development of a secure IT Infrastructure.

**2) Security for PC's and Laptops\*\* – 6 Days**

Due to the nature of the Broads Authority there is a significant amount of IT equipment being used in remote locations. These machines are at a greater risk of loss or damage than static machines and inevitably will hold some (if not large amounts of) data.

**3) Remote Access\* – 5 days**

Due to the distributed setup there are a number of remote users who need access to the Authority network on a regular basis. In addition Suppliers also need access to support the Authority applications. Failure to manage and control these users could leave the network open to attack.

**4) Network Domain Security\*\* – 8 Days**

The network enables users to connect to servers and equipment which is not directly connected to their own physical PC or workstation. This could be on the next desk (as in printers), other rooms, other buildings or even other countries depending on the type of network. This access is managed through the Domain Controller (DC) where the users rights to access the network are managed.

**5) Data Centre and Backups\*\* – 5 Days**

- Backup and Restore Arrangements;
- Physical Access and Controls; and
- Environmental Controls;

**6) Project Management – 10 days**

Project management is the discipline of organising and managing resources in such a way that these resources deliver all the work required to complete a project within defined scope, time, and cost constraints. This review will look at the project framework around IT projects within the Council and how the projects are controlled and the project risks managed.

---

### **7) Anti Virus\* – 6 Days**

Although there have been virus breaches in the past, Anti Virus products tend to be relatively robust, provided they are implemented on the machines correctly, and users cannot bypass the software and it is correctly configured to update. A virus or Spyware can have a significant impact on the IT systems infected and the network as a whole so may cause reputational damage if the Authority is infected.

#### **Applications:**

### **8) Document management (Sharepoint)\* – 8 Days**

This system is widely used within the Authority as a document management system and Document Library. If this resource is not appropriately managed and developed it could have a significant impact on the efficiency of the Authority to store and retrieve important documentation, or leave confidential data open for others to see.

### **9) HR Application (SnowDrop)\*\* – 8 Days**

The HR system contains more data about individuals working for the Authority than any other system, therefore failure to secure and manage the application and its data runs the risk that sensitive data could be lost, manipulated or stolen.

### **10) Toll Systems Application\*\*\* – 8 Days**

During key time periods this application is key to the Authority, during peak periods it processes details for £2,000,000 in tolls for 10,000 boat owners during the April rush. This application is in the process of being replaced which has not gone as smoothly as expected, therefore an Audit of the application approximately four months following implementation would provide assurance over the controls in place over the application once it is live.

## **7. AUDIT COVERAGE IMPLICATIONS FOR THE ANNUAL AUDIT PLAN FOR 2009/10 AND THE STRATEGIC AUDIT PLAN FOR 2009/10 TO 2013/14**

Upon receipt of the outcomes of the Computer Audit Needs Assessment work, the Head of Internal Audit has consulted with Broads Authority senior management and it has been that the Toll Systems Application be examined in 2009/10, whilst provisional acceptance has been given to audits of IT Governance and Strategy in 2010/11, followed by reviews of Network Domain Security plus Data Centre and Backups in 2011/12.

*APPENDIX 1 - Computer Audit Needs Assessment Results*

	<b>Risk Rating</b>	<b>Audit Number</b>	<b>Rationale</b>
<b>Network Based</b>			
Network Infrastructure	Low Risk		This is under contract from Defra who maintain the primary network, and the Broads Authority have responsibility for switches and policing.
Network Security	High Risk	4	High risk area, Network Security can be complex and failure to manage security could leave the network open to abuse.
Wireless Networks	Low Risk		Wireless networks are not in use at the Authority.
Remote Access (User)	Medium Risk	3	There are a number of remote users but if they could not connect they would be able to visit the office. The main risk here is the connection channels from outside the Authority.
Remote Access (Supplier)	Medium Risk	3	The Authority has a number of remote suppliers and if they could not connect they would be able to visit the office. The main risk here is the connection channels from outside the Authority.
Telecommunications/VOIP	Low Risk		There is a mix of telecoms and Voice Over IP (VOIP), if there were any issues most staff members also have mobile phones.
Content Management (Web site (Internet))	Low Risk		The website is externally hosted and editorial privileges are limited to one per department, in addition the Authority has just taken on a web manager.
Content Management (Web site (Intranet))	Low Risk		Sharepoint is used to manage separate document libraries, in addition the Authority has just taken on a web manager.
E-Mail	Low Risk		There is a lot of reliance placed on e-mail for storage of information and communication. The main risk here is a loss of data or the facility. Backups and recovery are key in this area.
Internet	Low Risk		Short periods of time without internet access would have little impact on the Authorities services.
Virus Protection/Spyware	Medium Risk	7	There have been a couple of infections over the last few years but the Authority now use SCM and ICM from computer associates, with regular updates.
<b>Security &amp; Control Reviews</b>			
Business Continuity	Medium Risk	N/A	This is not currently in place, but will be touched upon during the 08/09 Disaster Recovery Audit.
Disaster Recovery	Medium Risk	N/A	This is not currently in place, but will be covered during the 08/09 Disaster Recovery Audit.
Data Back-up	High Risk	5	Failure to backup could loose data if there were an issue.

	<b>Risk Rating</b>	<b>Audit Number</b>	<b>Rationale</b>
Data Centre	Medium Risk	5	This is a shared facility so we do not have full control over who has access.
Computer Room (Environmental Controls)	Medium Risk	5	This is a shared facility so we do not have full control over who has access.
<b>System Reviews</b>			
E-Procurement	Not Applicable		Not Used
E-Payments	Not Applicable		Not Used
Helpdesk	Low Risk		Service calls are logged in SharePoint.
PC End User controls	High Risk	2	There are a number of laptops in use, USB drives, etc. and the Broads Authority offices are part of a shared facility with no access controls against other companies in the facility
<b>Management Issues</b>			
Policy/ ISO27001/ITIL/ISO9000	High Risk		There are very few IT Policies in place
Governance	Medium Risk		The Authority is still small enough for IT to maintain good links with all departments and the structure has changed to accommodate the growth.
Project Management	Low Risk	6	The Authority has a project manager who looks after the projects for the Authority. Although the Authority undertakes a number of projects, they tend to bring in expertise for the implementation of new systems.
Software Licensing (inc FAST)	Low Risk		There is no software asset management system in place although because the Authority is classed in the education area they tend to obtain enough licences to cover most people. Deficiencies in licences will likely be due to people loading their own software, although this is low risk providing policies are in place.
Strategy	Medium Risk	1	There is an Authority Strategy in place however there is no specific IT Strategy in place.
Data Protection	Low Risk		The Authority has limited sensitive data and there is a DPA Officer.
Freedom of Information	Low Risk		The Authority has a freedom of information officer and much of the documentation is in the public domain, or stored within the Sharepoint Libraries.
IT Security (PC, Data, Asset, etc)	High Risk	2	There are a number of laptops in use, USB drives, etc and the Broads Authority offices are part of a shared facility with no access controls against other companies in the facility.

---

	<b>Risk Rating</b>	<b>Audit Number</b>	<b>Rationale</b>
Procurement/Acquisition	Low Risk		All ITC hardware and software is to be procured through ICT.
Change Control	Low Risk		The Authority currently use Sharepoint to log calls and manage changes, but the process and monitoring could be improved. Most applications are supported externally therefore any changes made are under guidance from suppliers.

*Appendix 2 – Recommendations arising as a result of the Needs Assessment*

During the Needs Assessment process Audit identified two areas of concern, which could put the security of the Authority’s data and IT systems at risk. We have therefore raised two recommendations for consideration prior to any IT Audit work commencing. These are detailed below.

**1. DragonFly House Office Security (High priority)**

Recommendation	Rationale
<p>Secure the Broads Authority Office area from unauthorised access by other organisations and visitors using the same building.</p>	<p>Protecting the Authority office areas from unauthorised access will help protect assets which are kept in the area overnight, including Data, PC’s and peripherals.</p> <p>Currently the offices in DragonFly house are not protected from other organisations, or their visitors using the same building as there are no physical barriers to manage traffic through the offices or prevent access after hours.</p> <p>The Authority data and assets are at risk where they are not appropriately secured.</p>

**2. Server Room Security (Medium priority)**

Recommendation	Rationale
<p>Appropriate cabinet locks should be fixed to the server racks as a matter of urgency.</p> <p>The ‘Head of IT and Collector Of Tolls’ should also obtain regular updates from the building management as to who has access to the server room.</p>	<p>Appropriate security over access to the Authority’s server racks should help prevent other users of the server room gaining unauthorised access to the Authority’s data, services or equipment.</p> <p>At the time of the needs assessment it was observed that the server racks had not been fully secured to prevent unauthorised access.</p> <p>The Authority data and assets are at risk where they are not appropriately secured.</p>

## Appendix 5

### Follow-up of Internal Audit recommendations at 31 March 2009

1. The Internal Audit Service provider, Deloitte and Touche Public Sector Internal Audit Ltd., undertakes a validation process to ensure that Internal Audit recommendations due at 31 March 2009 have been implemented, as agreed.
2. As at 31 March 2009, the following recommendations had been raised in relation to 2007/08 and 2008/09 audits:

<b>Audit No.</b>	<b>Description</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>Total</b>
BA/08/02	Development Control	0	1	4	5
BA/08/03	Key Controls	0	2	1	3
BA/09/01 Part 1	Corporate Governance	0	2	1	3
BA/09/01 Part 2	Annual Governance Statement	0	4	3	7
BA/09/02	Computer Audit Needs Assessment	1	1	0	2
BA/09/03	Toll Income	0	2	0	2
BA/09/04	Asset Management	1	4	1	6
BA/09/05	Payroll and HR	0	6	0	6
BA/09/06	Disaster Recovery	2	1	0	3
BA/09/07	Key Controls	0	5	3	8
	<b>Total</b>	<b>4</b>	<b>28</b>	<b>13</b>	<b>45</b>

3. The current position with regard to implementing the 45 recommendations is as follows:

<b>Status</b>	<b>High</b>	<b>Medium</b>	<b>Low</b>	<b>Total</b>
Completed / Superseded	0	9	6	15
Partly Implemented	0	0	0	0
Not Yet Implemented (as confirmed by management)	0	1	3	4
Not yet due for implementation	4	18	4	26
<b>Total</b>	<b>4</b>	<b>28</b>	<b>13</b>	<b>45</b>

4. As is demonstrated in the table above, all high priority recommendations that have been raised are not yet due for implementation until after 31 March 2009. The 26 recommendations not yet due for implementation will be reviewed as part of the follow-up process for next year.
5. The 4 recommendations due which have not yet been implemented are identified below.

<b>Audit – BA 08/02 Development Control</b>					<b>Report Issued - 01 Jul 08</b>
<b>Recommendation: 3 - Safe Access Code Change</b>					<b>Priority: Low</b>
The access code to the Finance Office safe should be changed periodically and the revised code should only be notified to authorised personnel.	It is agreed the safe access code should be changed periodically.	Initial Deadline: 31 Jul 08	Head of Finance	<b>Agreed</b>  <b>Outstanding</b>	May 2009  We confirmed from discussion with the Director of Corporate Services that this recommendation still remains outstanding but will be progressed by the Authority.

<b>Audit – BA 09/01 Corporate Governance Part 2</b>					<b>Report Issued - 01 Sep 08</b>
<b>Recommendation: 4 - External Partnership Protocols</b>					<b>Priority: Medium</b>
The External Partnership Protocols (Guidance for Officers) should be reviewed, amended where necessary and dated, on an annual basis.	The External Partnership Protocols (Guidance for Officers) will be reviewed, amended where necessary and dated, on an annual basis.	Initial Deadline: 01 Sep 08	Director of Corporate Services	<b>Agreed</b>  <b>Outstanding</b>	May 2009  We confirmed from discussion with the Director of Corporate Services that this recommendation still remains outstanding but will be progressed by the Authority.

<b>Audit – BA 09/01 Corporate Governance Part 2</b>					<b>Report Issued - 01 Sep 08</b>
<b>Recommendation: 6 - Fraud and Corruption Policy</b>					<b>Priority: Low</b>
The Fraud and Corruption Policy should be reviewed and updated, as appropriate, on an annual basis.	The Fraud and Corruption Policy will be reviewed and updated, as appropriate, on an annual basis.	Initial Deadline: 01 Sep 08	Director of Corporate Services	<b>Agreed</b>  <b>Outstanding</b>	We confirmed from discussion with the Director of Corporate Services that this recommendation still remains outstanding but will be progressed by the Authority.

<b>Audit – BA 09/01 Corporate Governance Part 2</b>					<b>Report Issued - 01 Sep 08</b>
<b>Recommendation: 7 - Action Plan</b>					<b>Priority: Low</b>
The Annual Governance Statement 2007/8 action plan compiled by the Authority as a result of the Annual Governance Statement should list the priority of each action point.	Priority ratings will be given to each action point.	Initial Deadline: 01 Aug 08	Director of Corporate Services	<b>Agreed</b>  <b>Outstanding</b>	April 2009  As part of BA 10/01 it was noted that priority ratings were not recorded against the actions for the AGS action plan 2007/08.

