Financial Scrutiny and Audit Committee
10 July 2012
Agenda Item No 7

Internal Audit Annual Report and Opinion 2011/12

Report by Head of Internal Audit

Summary: This report has been developed to satisfy the requirements of the Accounts and Audit Regulations 2011 'to undertake an adequate and effective internal audit of the organisation's accounting records and of its system of internal control in accordance with the proper practices in relation to internal control', and to meet the Head of Internal Audit's annual reporting obligations as set out in the CIPFA Code of Practice for Internal Audit in Local Government. To confirm that the organisation has complied with the above, the Head of Internal Audit has produced an Annual Report and Opinion, which examines and utilises the outcomes of Internal Audit Work undertaken in both 2011/12 and 2012/13 to formulate an opinion on the overall internal control environment which has been operating at the Authority over the last twelve months.

Recommendation:

That the Committee is requested to:

(i) receive and note the Annual Report of the Head of Internal Audit;
(ii) note the overall standards of internal control were adequate for the year ended 31 March 2012;
(iii) note that a good assurance has been given in respect of Corporate Governance arrangements and systems of Risk Management for the year ended 31 March 2012; and
(iv) note that the opinions expressed together with other matters arising from internal audit work have been given due consideration when developing the Authority's Annual Governance Statement.

1 Introduction

1.1 The CIPFA Code of Practice for Internal Audit in Local Government in Section 10.4 stipulates that the Head of Internal Audit should report the following information at least annually:

- An opinion on the overall adequacy and effectiveness of the organisation's internal control environment.
- Any qualifications to that opinion, together with the reason for qualification.
- A summary of the audit work from which that opinion was derived.
- Any issues considered relevant to the Annual Governance Statement.

- Comparison of actual audit work undertaken with planned work, summarising the performance of internal audit against its performance measures and targets.
- Commentary on compliance with the standards of the Code of Practice for Internal audit.
- Communication of the results of the Internal Audit quality assurance programme.

1.2 This report therefore seeks to address the key items specified above, although recognising that some aspects are covered in an additional report, i.e. an evaluation of the performance of the Internal Audit Service is subject to separate reporting, and will feature in a report headed up 'Annual Review of the Effectiveness of Internal Audit'.

1.3 Within this Committee agenda, it is further acknowledged that the Director of Change Management and Resources will also be providing a more up-to-date position statement on the status of audit recommendations. The Head of Internal Audit's Annual Report will additionally revisit the year end situation concerning the implementation of agreed audit recommendation, based on verification work undertaken in Quarter 4 of 2011/12.

2 Internal Audit Service Provisions and Costs

2.1 The Internal Audit Service arrangements at the Broads Authority have remained unchanged throughout 2011/12, in so far as the Head of Internal Audit of South Norfolk Council has continued to be responsible for managing the delivery of the Internal Audit Service to the organisation and controlling the work of Deloitte Public Sector Internal Audit Ltd, which is contracted to deliver the programme of work as detailed in the Annual Audit Plan.

2.2 The fees associated with the provision of the Internal Audit function to the Authority during 2011/12 comprise two distinct elements namely: input by the Internal Audit Services contractor to undertake the planned audit assignments earmarked for delivery in 2011/12; and the level of support required from the Audit Management Team to oversee all aspects of the service provision to officers and members. The cost of the service provision has been as follows:

Nature of the work	**2010/11 £**	**2011/12 £**
Cost of the planned work (Deloitte)	£9,504	£11,722
Cost of managing the service, supporting the Audit Committee and officers (South Norfolk Council)	£4,225	£3,360
TOTAL COST	**£13,729**	**£15,082**

2.3 The adoption and subsequent completion of a larger Audit Plan in 2011/12, compared with the previous year, is the main reason why costs have risen year on year. The 2011/12 Plan required delivery of 37 days split over five separate audit assignments, whereas 2010/11 planned provisions entailed 30 days to undertake three individual audits. It should be noted that an element

of the 2011/12 fees was prepaid in 2009/10 to fund the Toll Income Application audit. This could not actually be undertaken until two years later than first envisaged due to problems with the development and roll out of the new Tolls Management System.

2.4 The costs associated with Audit Management Team input have conversely reduced, in spite of the fact that there has been a greater number of assignments requiring officer input and, in addition, the Head of Internal Audit participated in a Risk Management Workshop and the National Parks Authority Performance Assessment in the course of the year.

3 Opinion of the Head of Internal Audit on the Overall Adequacy of the Internal Control Environment at the Broads Authority

3.1 The overarching opinion contained within this report relates to the system of internal control at the Authority and the overall control environment in place.

3.2 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.

3.3 The control environment encompasses the systems of corporate governance, risk management and internal control, hence, the Head of Internal Audit's Annual Opinion focuses on the effectiveness of the control environment based on an assessment of these systems, in line with areas targeted for audit focus in the approved Annual Audit Plan for 2011/12.

3.4 In order to be able to give an overall opinion, the Head of Internal Audit has taken into account the assurance levels given to individual audit assignments completed in respect of 2011/12 and, from this body of work, has confirmed **it is my opinion that the overall standards of internal control are adequate at the Broads Authority for the year ended 31 March 2012**. This opinion is in accordance with the definitions provided at Appendix 3 and is derived from the audits recorded in Appendix 1, whilst their corresponding Management Summaries are attached at Appendix 2**.** A more detailed narrative on audit outcomes is included within Section 5 of the report.

4 Basis of Assurance

4.1 To reiterate, all audits have been performed in accordance with mandatory standards and good practice set out within the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom, the specifications stated in the Internal Audit Services Contract between South Norfolk Council and Deloitte Public Sector Internal Audit Ltd, plus the standards laid down by Deloitte's own internal quality assurance systems.

4.2 Furthermore, all audit work has been cognisant of the principal risks identified in the Authority's Strategic Risk Register (details of which were used to develop the Annual Audit Plan for 2011/12) and changing priorities/additional requirements arising during the year.

5 The Nature of Audit Work from which the Opinion is Derived

5.1 System of Internal Control

5.1.1 We have undertaken three assignments in year scrutinising the Authority's systems of internal control applying to Planning, Key Financial Controls and the Toll Income Application. A study of the first two areas resulted in the award of adequate assurance levels but the Toll Income application highlighted a number of issues in its parallel running phase, culminating in the giving of a limited opinion and the development of nine audit recommendations, all of which were subsequently accepted by management.

5.1.2 In the course of our work during 2011/12, there have been two significant matters arising, with management being advised immediately of issues which were found to be undermining the Authority's systems of internal control. The first concerned password controls linked to the new Toll Income system. We raised a high priority recommendation that management should work with the developer of the Tolls Management System to strengthen password controls to current good practice standards. Management dealt with this issue as soon as it was brought to their attention and resolved the matter prior to the release and circulation of the final audit report.

5.1.3 The second item became apparent when carrying out our Key Control testing work in Quarter 4 of 2011/12. An inspection of the two bank account reconciliations in April and October 2011 confirmed that the independent review of these had been delayed on one occasion. We thus performed more testing concerning the regularity with which independent reviews were carried out in year, and established that the Head of Finance had completed examinations of the bank account reconciliations for July, August, September, October, November and December 2011 but all at the same time, namely at the end of December. We therefore put forward a high priority recommendation to address this matter, prompting the Head of Finance to carry out reviews of monthly bank account reconciliations in a more appropriate timely manner. Management responded by agreeing to schedule independent monthly reviews of completed bank account reconciliations in the future, and subsequent audit verification work has confirmed this is now happening.

5.1.4 The satisfactory implementation of the two high priority recommendations mentioned at paragraphs 5.1.2 and 5.1.3 and the fact that there are no additional high priority recommendations, which require action in 2012/13, have also been acknowledged when awarding the Broads Authority with an adequate opinion with reference to its internal control environment.

5.2 **Implementation of Audit Recommendations**

5.2.1 As mentioned above in paragraph 1.3, the Committee is regularly updated as to the status of agreed audit recommendations by the Director of Change Management and Resources. However, this report specifically revisits the year end position, and upon completion of audit verification work, we have been able to confirm the following:

Recommendation status at:	**31/03/11**		**31/03/12**	
	No.	**%**	**No.**	**%**
Due for implementation	27		21	
Completed/ Superseded	20	74%	12	57%
Partly implemented	0	0%	5	24%
Outstanding	7	26%	4	19%
Unable to confirm status	0	0%	0	0%

5.2.2 The table demonstrates that management have been progressing audit recommendations although the percentage of fully completed/ superseded recommendations has fallen compared with the previous financial year. Nevertheless, there has been activity in relation to 81% of those recommendations that were due to be progressed in year, which strongly indicates that management are taking a proactive stance to resolve the internal control weaknesses highlighted in internal audit reports.

5.2.3 The five partly completed audit recommendations have medium priority ratings and the reviews to which they relate are noted in the table at Appendix 4(1) whilst more detailed information is provided on both partly implemented and outstanding recommendations at Appendix 4(2).

5.3 **Corporate Governance and Risk Management**

5.3.1 We have additionally undertaken an audit of the Authority's Corporate Governance and Risk Management arrangements for 2011/12 as part of the 2012/13 Annual Audit Plan. The findings of our review are attached at Appendix 2(4). With regard to the provisions in place**, I am able to give a good opinion in relation to Corporate Governance and Risk Management arrangements.** This represents a noticeable improvement on the previous year, when an adequate assurance was awarded.

6 Issues considered relevant to the Annual Governance Statement

6.1 As noted previously in the report, there are presently no outstanding high priority audit recommendations. Moreover, in the majority of areas subject to audit inspection we have been able to provide positive assurances on conclusion of our work. However, there was one area where we were

obliged to give a less favourable limited assurance and this affected the Toll Income Application. Since there are six medium recommendations currently outstanding; reference to this audit should be considered when formulating the Authority's Annual Governance Statement.

7 Comparison of Planned and Actual Audit Work Undertaken

7.1 There were no major changes to the composition of the Annual Audit Plan for 2011/12. However, there were some instances where the rescheduling of work proved necessary. All revisions to our original timetable for delivering audits were agreed with management and are noted in Appendix 1.

8 Completion of Computer Audit Needs Assessment

8.1 The other key piece of work delivered in 2011/12 was a Computer Audit Needs Assessment. Due to the limited time available in Annual Audit Plans to undertake work of this specialised nature and based on the risk profile of IT auditable areas, three areas were subsequently put forward for management's agreement, one constituting a 'reserve' audit. However, in view of the considerable pressures on the Authority's ICT Team in 2012/13, there has since been a request from management to defer these particular audits to 2013/14 onwards. Furthermore, bearing in mind that there may be different/additional risks at that time, it may be necessary to undertake a short reassessment of the risks in early 2013/14, to take into account any changes in circumstances, before confirming which audits should be commissioned. The report containing the findings of the Computer Audit Needs Assessment can be found at Appendix 5.

Background Papers:	None
Author:	Sandra King, Head of Internal Audit
Date of Report:	26 June 2012
Broads Plan Objectives:	None
Appendices:	APPENDIX 1(1) Review Work delivered in accordance with the Annual Audit Plan for 2011/12 APPENDIX 1(2) Review Work delivered in accordance with the Annual Audit Plan for 2012/13 APPENDIX 2 - Management Summaries in respect of Completed Audit Assignments APPENDIX 3 - Definitions/Categories of Audit Opinions APPENDIX 4(1) - Summary of Agreed Audit Recommendations as at 31 March 2012 APPENDIX 4(2) - Outstanding Audit Recommendations as at 31 March 2012 APPENDIX 5 - Computer Audit Needs Assessment Report

Appendix 1 (1)

Review Work delivered in accordance with the Annual Audit Plan for 2011/12

Audit No.	Description of Audit	Frequency of Audit Coverage	Original Planned Days	Revised Days Planned	Days Delivered	Original Scheduling	Status	Assurance Level applicable	Summary Report Details presented to Members
BA/12/01	Corporate Governance and Risk Management	Annual	5	5	5	April	**Complete** **Final Report issued 17 May 2011**	Adequate	Financial Scrutiny and Audit Committee 12 July 2011
BA/12/02	Key Controls, Assurance Work and Follow Up	Annual	15	15	15	February	**Complete** **Final Report issued 11 April 2012**	Adequate	**Financial Scrutiny and Audit Committee 10 July 2012**
BA/12/03	Planning	4-yearly	7	7	7	~~October~~ August	**Complete** **Final Report issued 13 October 2011**	Adequate	**Financial Scrutiny and Audit Committee 10 July 2012**
TOTAL PLANNED SYSTEMS AUDIT WORK			**27**	**27**	**27**	**100%**			
PLANNED COMPUTER AUDIT WORK									
BA/12/04	Toll Management System Application	Deferred from 2009/10 Annual Audit Plan	7	7	7	~~September~~ November	**Complete** **Final Report issued 9 December 2011**	Limited	**Financial Scrutiny and Audit Committee 10 July 2012**
BA/12/05	Computer Audit Needs Assessment	3-yearly	3	3	3	~~November~~ January	**Complete** **Final Report issued 23 April 2012**	Not Applicable	**Financial Scrutiny and Audit Committee 10 July 2012**
TOTAL PLANNED COMPUTER AUDIT WORK			**10**	**10**	**10**	**100%**			
TOTAL PLANNED WORK			**37**	**37**	**37**	**100%**			

Appendix 1 (2)

Review Work delivered in accordance with the Annual Audit Plan for 2012/13

Audit No.	Description of Audit	Frequency of Audit Coverage	Original Planned Days	Revised Days Planned	Days Delivered	Original Scheduling	Status	Assurance Level applicable	Summary Report Details presented to Members
BA/13/01	Corporate Governance and Risk Management	Annually	5	5	4	April	Complete Final Report issued 1 May 2012	Good	**Financial Scrutiny and Audit Committee 12 July 2012**
BA/13/02	Key Controls and Assurance	Annually	15			January			
TOTAL PLANNED SYSTEMS AUDIT WORK			**20**	**5**	**4**				
PLANNED COMPUTER AUDIT WORK									
BA/13/03	Computer Audit Project - Details to be confirmed		7	0	0	October	Audit deferred to 2013/14 at the request of management		
TOTAL PLANNED COMPUTER AUDIT WORK			**7**	**0**	**0**				
TOTAL PLANNED WORK			**27**	**5**	**4**				

APPENDIX 2

Management Summaries in respect of Completed Audit Assignments

Report No. BA/12/02 – Final Report issued 13 October 2011

Audit Review of Planning

Audit Opinion

Adequate Assurance given

Rationale supporting award of audit

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 was audited previously by Deloitte in July 2008. The level of assurance remains unchanged since the last visit.

Summary of Findings

Planning Applications

Controls are in place over the receipt, validation, and the decision-making process for planning applications. Formal review of the policies and working instructions for planning, enforcement and appeals should be undertaken on a regular basis and this has not occurred since March 2007. There is also a requirement for additional controls to be introduced over the verification of planning fee income received.

Enforcement

Policy and standards are in place with respect to enforcement, although as stated above, there is a requirement for these to be reviewed and updated to bring them in line with current working practices.

Controls are in place over the monitoring and progression of enforcement cases and the Planning Committee are updated with progress reports as required.

Appeals

A documented procedure is in place with regard to appeals which also requires review and update. Applicants are made aware of their right to appeal. Appeals are reported to the Planning Committee on a monthly basis.

Performance Information

Performance indicators have been set by the Authority and these are monitored on a quarterly basis, with results being presented to the Planning Committee.

Risk Management

There are no risks in the Strategic Risk Register specifically relating to development control, although a number of risks have been identified that apply. There are mitigating actions in place for each risk, with owners having been assigned and controls in place over the periodic review of risks and mitigation.

The following number of recommendations has been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	**Medium**	**Low**
	Planning Applications	Amber	Amber	0	2	0
	Enforcement	Green	Green	0	0	0
	Appeals	Green	Green	0	0	0
	Performance Information	Green	Green	0	0	0
	Risk Management	Green	Green	0	0	0
Total				**0**	**2**	**0**

High Priority Recommendations

We have not raised any high priority recommendations as a result of this audit.

Management Responses

Management have accepted the recommendation raised.

Report No. BA1204 – Final Report issued 9 December 2011

Audit Review of Tolls Management System/Application

Audit Opinion

Limited Assurance given

Rationale supporting 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.
- Although one High Priority and eight Medium Priority recommendations have been raised, a number of controls were found to be in place and operating effectively.
- Recommendations have been raised to help strengthen these controls to a good/leading practice and help mitigate against risks where the controls were seen to be weak. However, we have concerns around the password controls, especially given the imminent live implementation of the application. As such, we are only able to provide a limited level of assurance.

Summary of Findings

Access Controls

There are good controls in place around segregation of access privileges and there is good evidence of robust system administration cover. However, there are serious weaknesses concerning the lack of password controls. It was also found that passwords could be viewed on screen in clear text. Recommendations on these weaknesses have been raised.

Data Input

The application was found to have good controls with respect to capturing bad data on input. Customer documentation is scanned when they have been input, whereupon the originals are destroyed. However, it was found that, although customer credit card data is being obscured before the scans are made, the data is still visible. A recommendation on this has been raised.

Data Processing

There are good controls in this area. Processing consists of the need to create batches of input data, with the number of batches being created each day dependant on workload.

Data Output

We noted good controls in this respect in terms of reconciling data from input to output, with good evidence of management review at each stage. There is little need for routine distribution of management reporting and they are all available electronically if required.

Interfaces

There is an interface with the Dimensions Finance system and also with the proposed online payments system, which is currently under test. Testing of both interfaces suggest that good reconciliation controls are in place. The online service has not yet undergone stress testing to provide assurance over its ability to service customer applications at peak times, which is during March, although activity tends to increase from February as renewal notices are sent out. A recommendation to investigate available options in this respect has been raised.

Backups

The application and data is backed up each day to disc and tape. Tapes are taken home by staff

each evening and then returned the following day. This presents a risk to personal safety and data breaches if the tapes are stolen or lost. In addition, during the day, both the tapes and disc backups are on site, which means that if the office cannot be accessed for an extended period after the tapes are returned, recovery to an alternate site will not be possible. There is a potential weakness concerning database housekeeping in that it is clear that certain Oracle jobs are running, although they are not being closely managed. Business Continuity and Disaster Recovery Plans should also be reviewed. Recommendations to help lift these areas have been raised.

Support and Maintenance

Whilst there is external support in place, it is not yet formalised and a recommendation to resolve this has been raised. Whilst the audit noted good change control processes that use SharePoint, a recommendation has been raised to ensure that there is a distinction between the implementation project and the live system.

The following number of recommendations has been raised:

Adequacy and Effectiveness Assessments	**Area of Scope**	**Adequacy of Controls**	**Effectiveness of Controls**	**Recommendations Raised***		
				High	**Medium**	**Low**
	Access Controls	Amber	Amber	1	1	0
	Data Input	Amber	Amber	0	1	0
	Data Processing	Green	Green	0	0	0
	Data Output	Green	Green	0	0	0
	Interfaces	Amber	Amber	0	1	0
	Backups	Amber	Amber	0	3	0
	Support and Maintenance	Amber	Amber	0	2	0
Total				**1**	**8**	**0**

High Priority Recommendations

We have raised one high priority recommendation as a result of this audit. This is in the following area:

Access Controls - User Identification

Management should work with the developer of the Tolls Management System to strengthen password controls to current good practice standards including:

- Implementing a minimum of seven characters;
- Enabled and enforced password complexity;
- Regular change periods of 30-90 days; and,
- Lockout following three unsuccessful access attempts.

Ideally, the enhancements should include the ability to report bad password attempts to system administrators within the audit logs.

Management Responses

Management have accepted both recommendations raised.

Report No. BA1205 – Final Report issued 11 April 2012

Audit Review of Key Controls

Audit Opinion

Adequate Assurance given

Rationale supporting 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 level of assurance is based on the fact that we have raised one high, two medium and one low priority recommendations which relate to the need for prompt reviews of bank account reconciliations, to retain evidence of the annual reconciliation of the asset register, the formulation and retention of a budget setting timetable and a review of the authorised signatory list for approving expenditure.
- An audit of this area was previously carried out in 2010/11 when an Adequate Assurance opinion was given.

Summary of Findings

Treasury Management/Investments

Broadland District Council manages the Authority's investments on its behalf. Investments proposed by the Senior Finance Assistant following the production of a weekly cash flow statement are in accordance with the Investment and Capital Financing Strategy 2011/12 and are authorised by the Head of Finance. Reconciliations with the general ledger are independently reviewed by the Head of Finance. A summary of investments is reported to the Financial Scrutiny and Audit Committee on an annual basis.

Main Accounting System/General Ledger

Bank reconciliations and reconciliations of the purchase and sales ledgers with the general ledger are independently reviewed by the Head of Finance. Reviews of bank reconciliations had been delayed with the Head of Finance having reviewed a period of six months in December 2011.

Suspense accounts are investigated and cleared on a monthly basis. The general ledger system does not allow an imbalanced journal to be processed. Journals and adjustments for posting on to the ledger are retained with supporting documentation. Processing is restricted to staff in the Finance Department.

Fixed Assets

The fixed asset register is retained on a shared drive with access restricted to staff in the Finance Department. Fixed assets exceeding £5,000 are originally valued at their historic cost and then re-valued on a five yearly basis. The appropriate valuation and depreciation costs are updated on an annual basis.

The Head of Finance was unable to locate any evidence to confirm that the asset register had been reconciled at the end of 2010/11.

Budgetary Control

Budgets are set in accordance with an agreed timetable, considered by the Navigation Committee and formally approved by the Broads Authority. The Director of Change Management and Resources was unable to locate a copy of the budget setting timetable for 2011/12. However, we were able to confirm that the budget for 2011/12 had been approved by the Broads Authority in March 2011.

Once the budgets are set, they are profiled following budget manager input and entered on to the general ledger. Budget holder responsibility is identified in the Budget Book 2011/12.

Comments received from budget holders following the receipt of monthly budget statements relating to variances over £10,000 are included in a monthly Summary of Major Variances report for review by senior management. However, a report had not been produced for October 2011 due to other work commitments, although this was considered to be an isolated incident and as such, no recommendation is deemed necessary.

The Navigation Committee, which meets six times during the year, considers the budget monitoring report as a standing agenda item.

Creditors/Purchase Ledger

Orders are subject to approval by an authorised signatory in accordance with delegated limits. However, it was identified that there were instances where the details of the persons authorising the order did not appear on the authorised signatory list. Subsequent confirmation was obtained that the persons signing these orders did have the requisite levels of authority to approve these orders.

When an invoice is received, it is scanned and matched to the original order and authorisation is requested. Goods or services received are confirmed before being certified for payment.

A manual list of the invoices in a batch is produced and reconciled to the purchase ledger and independently reviewed. Weekly reconciliations are completed between the approved invoices and payments on the purchase ledger which are independently reviewed.

Debtors/Sales Ledger

Batch reports are included as part of the monthly bank reconciliation process which includes reports of all the payments received and made throughout the month.

An aged debtors list is produced on a monthly basis as part of the reconciliation process and outstanding payments reviewed. Reminder letters are issued for invoices outstanding after 30 days with the aged debtors list updated to document the recovery steps taken.

Payroll

Additions to the payroll are documented on a new starter form approved by the HR Officer who maintains a new starter checklist. Evidence supporting leavers, including copies of the resignation letters is retained.

Evidence of any authorised payroll amendments is also retained. Payroll forms are sent to the Payroll Co-ordinator at Broadland District Council for processing.

Staff at the Broads Authority do not have any involvement in the production and authorisation of the payroll, although a check is undertaken of the payroll information in respect of reconciling the invoice received from Broadland District Council and the ledger following the payment run.

The Senior Finance Assistant and Human Resources Officer undertake an annual review of the Authority's establishment.

Toll Income

Toll charges are levied and reviewed by the Navigation Committee on an annual basis before being formally approved by the Broads Authority. Charge notifications are printed mid-February and sent out to applicants over the subsequent four week period in advance of the new year period.

The notifications issued are reminders and are enforceable should boat users use the Broads without the required license. The HARPS (Tolls Management) system is reconciled to the general ledger on a monthly basis and any discrepancies are investigated. There is a segregation of duties in place as members of the Tolls Team collect income and the recording of income is undertaken by the Assistant Collector of Tolls.

Follow Up

All outstanding recommendations where an implementation deadline prior to 31st March 2012 had been agreed were subject to review. The following summary provides details of our findings as a result of this audit:

The following number of recommendations has been raised:

Adequacy and Effectiveness Assessments	**Area of Scope**	**Adequacy of Controls**	**Effectiveness of Controls**	**Recommendations Raised***		
				High	**Medium**	**Low**
	Treasury Management /Investments	Green	Green	0	0	0
	Main Accounting System/General Ledger	Green	Amber	1	0	0
	Fixed Assets	Green	Amber	0	1	0
	Budgetary Control	Green	Amber	0	0	1
	Creditors/Purchase Ledger	Green	Amber	0	1	0
	Debtors/Sales Ledger	Green	Green	0	0	0
	Payroll	Green	Green	0	0	0
	Toll Income	Green	Green	0	0	0
Total				**1**	**2**	**1**

High Priority Recommendations

We have raised one high priority recommendation as a result of this audit. This is in the following area:

Main Accounting System/General Ledger

Monthly bank account reconciliations should be undertaken in a timely manner and subject to independent review.

Management Responses

Management have accepted both recommendations raised.

Report No. BA/1301 – Final Report issued 1 May 2012

Audit Review of Corporate Governance and Risk Management

Audit Opinion

Good Assurance given

Rationale supporting award of opinion

The audit work carried out by Internal Audit indicated that:

- There is a sound system of internal control designed to achieve the client's objectives.
- The control processes tested are being consistently applied.
- This opinion results from the fact that we have raised one low priority recommendation.
- The level of assurance has improved since the previous visit.

Summary of Findings

Corporate Governance

The two key governance documents within the Authority are the Code of Corporate Governance and Scheme of Delegation. The Code of Corporate Governance is reviewed on an annual basis with the most recent review having been undertaken in May 2011.

Minor amendments were made to the Scheme of Delegation as a result of organisational changes to directorates during 2011/12, which have been approved by the Broads Authority. A full review is to take place during 2012/13 as part of the three-yearly policy review cycle.

Both the Code of Corporate Governance and the Scheme of Delegation have been updated to reflect organisational changes, including directorate positions and associated delegations.

Training needs of staff are incorporated within annual corporate and directorate training plans. These cover day-to-day training needs as well as 'essential' training regarding key changes to governance structures within the Authority during 2011/12. Progress of 'essential' training plans is reported to members through the Strategic Priorities report presented at each bi-monthly Authority meeting.

Members are provided training in the Code of Conduct during the induction process.

Risk Management

The Broads Authority has a Risk Management Policy which has been approved by the Financial Scrutiny and Audit Committee during 2011/12.

A Strategic Risk Register is in place which documents risks to the Authority Risk assessments are undertaken for all new risks which includes scoring each risk in terms of impact and likelihood. Risk scores along with mitigating actions to reduce the impact and likelihood of risks are recorded on the Strategic Risk Register for each risk. Where appropriate, additional actions to further reduce the impact and likelihood of risks are defined on the register. Target dates for completion of additional actions had been exceeded in some instances.

Each risk has been assigned to a risk owner on the Strategic Risk Register. Risk owners are required to review risks on at least a six-monthly basis. Risk owners are to confirm the completion of these reviews to the Director of Change Management and Resources.

The following number of recommendations has been raised:

Adequacy and Effectiveness Assessments	Area of Scope	Adequacy of Controls	Effectiveness of Controls	Recommendations Raised		
				High	Medium	Low
	Corporate Governance	Green	Green	0	0	0
	Risk Management	Green	Amber	0	0	1
Total				**0**	**0**	**1**

High Priority Recommendations

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

Management Responses

Management have accepted the recommendation raised.

APPENDIX 3

Definitions / Categories of Audit Opinions

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

Good Assurance	There is a sound system of internal control designed to achieve the client's objectives. The control processes tested are being consistently applied.
Adequate Assurance	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.
Limited Assurance	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.
Unsatisfactory Assurance	Control processes are generally weak leaving the processes/systems open to significant error or abuse. Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.

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.

Summary of Agreed Audit Recommendations as at 31 March 2012

			Completed during 2010/11			Completed during 2011/12			Partly Implemented			Outstanding			Not yet due to be implemented			Total
Reference	**Description**	**Opinion**	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**	**H**	**M**	**L**	
BA/09/01 (2)	Annual Governance Statement	Adequate												1				**1**
BA/09/03	Toll Income	Adequate											1					**1**
BA/09/04	Asset Management	Adequate	1	3	1													**5**
BA/09/05	Payroll and Human Resources	Adequate		1														**1**
BA/09/06	Disaster Recovery	Limited	1	1														**2**
BA/10/01	Corporate Governance (08/09)	Limited						1										**1**
BA/10/02	Partnership working	Limited		1														**1**
BA/10/03	Key Controls (09/10)	Adequate		2	1													**3**
BA/10/04	Fen Ecological Project	Adequate		1	3													**4**
BA/11/01	Corporate Governance (09/10)	Adequate		3	1			1										**5**
BA/11/02	Key Controls (10/11)	Adequate					1											**1**
BA/11/03	IT Governance	Adequate					2							1				**3**
BA/12/01	Corporate Governance (10/11)	Adequate					2											**2**
BA/12/02	Planning	Adequate					1			1								**2**
BA/12/04	Toll Application	Limited				1	2			4			1			1		**9**
BA/12/05	Key Controls (11/12)	Adequate				1										2	1	**4**
			2	**12**	**6**	**2**	**8**	**2**	**0**	**5**	**0**	**0**	**2**	**2**	**0**	**3**	**1**	**45**

Outstanding Audit Recommendations as at 31st March 2012

Responsibility	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
Director of Change Management and Resources	Low	BA/09-01 – Annual Governance Statement – recommendation 6 The Fraud and Corruption Policy should be reviewed and updated, as appropriate, on an annual basis.	*Original Deadline:* September 2008 *Previous Revised Deadlines:* 31 May 2009, 31 December 2010	30 April 2012	Not yet implemented due to other priorities.	The Director of Change Management & Resources confirmed that this would be completed by the end of April 2012.
Head of ICT and Collector of Tolls	Medium	BA/09-03 – Toll Income – recommendation 1 Management should compile written procedures for all aspects of toll income, e.g. identification, receipt, banking and the collection of unpaid tolls, including timescales for taking action.	*Original Deadline:* August 2009 *Previous Revised Deadlines:* 30 July 2010, 31 December 2010	Not stated	Still outstanding pending completion of the Tolls Management System. However good progress is being made on this and the system is now almost ready for implementation in February 2012. Once the final system is delivered it will be possible to draw up the detailed policies and procedures.	The Head of IT & Tolls confirmed that this had been postponed pending the launch of the new Toll Management System at the beginning of 2012/13.
Head of ICT and Collector of Tolls	Low	BA/11-03 – IT Governance and Strategy – recommendation 2 Management should ensure that the minor changes that certain job descriptions require are implemented as soon	*Original Deadline:* 31 March 2011	30 June 2012	Still outstanding. A more significant change to job roles is required as a result of the decision to make one post	The Head of IT & Tolls confirmed that this would be implemented by the end of

Responsibility	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
		as possible.	*Previous Revised Deadlines:* 1 January 2012		redundant on 30 April 2011.	June 2012.
Head of Development Management	Medium	BA/12-02 – Planning – recommendation 1 All planning policies and work instructions should be reviewed and updated to take account of current working practices, responsibilities and the functionality enabled by the CAPS planning system. Documents should be subject to periodic review.	*Original Deadline:* 31 March 2012	30 April 2012	A review of all policies and working practices is underway, and will be recorded.	The Head of Development Management confirmed that this was underway and would be completed by the end of April 2012.
Head of IT and Collector Of Tolls	Medium	BA/12-04 – Toll Management System – recommendation 4 Management should look at implementing a programme of stress tests against the online payments process, or gain assurance from the supplier that the implementation will function within acceptable tolerances under expected current and future peak loads.	*Original Deadline:* 31 January 2012	Not stated	Volunteers are being sought to undertake stress testing of the new system.	The Head of IT & Tolls confirmed that this was underway. Stress testing was completed in February 2012 and implemented in the new year.
Head of IT and Collector Of Tolls	Medium	BA/12-04 – Toll Management System – recommendation 5 Management should explore the Oracle database management and housekeeping functionality to better understand and implement database housekeeping jobs. These should be run on a periodic basis as part of a wider	*Original Deadline:* 31 December 2011	30 April 2012	Current integrity tasks will be confirmed, monitored and extended as required.	The Head of IT & Tolls confirmed that this would be completed by the end of April 2012.

Responsibility	Priority	Recommendation	Deadlines	New Target Deadline	Current Response	Current Audit Comment
		database management routine.				
Head of IT and Collector Of Tolls	Medium	BA/12-04 – Toll Management System – recommendation 6 Management should review the process that takes backup tapes home overnight.	*Original Deadline:* 29 February 2012	Not stated	Officers will investigate options for the offsite storage of backup tapes. The Corporate IT Group will be consulted on this at its meeting on 27 January 2012.	The Head of IT & Tolls confirmed that the Corporate IT Group would be considering this on 27 January 2012.
Head of IT and Collector Of Tolls	Medium	BA/12-04 – Toll Management System – recommendation 8 Management must ensure that the current support arrangements are formalised and signed off as soon as possible, and no later than the go live date.	*Original Deadline:* 31 December 2011	30 April 2012	This is being pursued with the supplier, who has been requested to provide a copy of the Service Level Agreement as agreed in 2007.	The Head of IT & Tolls confirmed that this was in progress and would be completed by April 2012.
Head of IT and Collector Of Tolls	Medium	BA/12-04 – Toll Management System – recommendation 9 Management should ensure that adequate change control processes are put in place to manage changes within the Tolls Management System once it has gone live. These processes can mimic the existing SharePoint processes that the implementation project has put in place and should include back out plans should any implemented change fail.	*Original Deadline:* 31 January 2012	30 April 2012	A new Change Management Log will be created to record changes requested after the system has gone live, with the previous change log being archived.	The Head of IT & Tolls confirmed that this was in progress and would be completed by April 2012.

COMPUTER AUDIT NEEDS ASSESSMENT

Broads Authority

April 2012

BA/12/03

CONTENTS

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 corporate 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 ICT and Collector of Tolls. These discussions, along with the Authority's corporate 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, by the Secretary of State for the Environment and from the Authority's Navigation Committee.

The Broads Priorities 2009/10 - 2011/12 can be found on their website and include (amongst others):

- implement an integrated approach (0-20 years) to the management of the Broads landscape;
- work with the boating community & local organisations to provide a safe environment for navigation;
- 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 through effective partnership working; and
- implement actions to reduce the Authority's 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

At peak times the IT systems support up to 120 users, which include permanent and seasonal staff in services such as information centres. There are approximately 120 Permanent employees and 22 Seasonal employees working across three main sites and seven other remote locations. Approximately 88 Core users are based in Dragonfly House, 10 use the Ludham offices which are in the process of being vacated, 6 users are based at the Dockyard; and 4 users work out of the Beccles site.

Remote sites are connected via Virtual Private Networks (VPN) with Domain controllers at Dragonfly house, Ludham and Beccles. Plans have been submitted to extend the facility at the Dockyard which will allow a backup server room to be implemented as a warm backup site along with a domain controller.

Risk Register:

There is a Corporate Risk Register at the Authority and the main IT risk has been highlighted as 'Loss of IT/ Communications Systems', however, there were a number of other risks which could impact on IT. It was also noted that whilst the main IT risk covers almost all the IT infrastructure there was no mention of Data (Confidentiality, integrity or availability) which is the underlying purpose for IT provision. This risk has, however, been included as part of the Computer Audit Needs Assessment process, although not documented as such in the appendices.

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) – (Tolls Management System (TMS)) – audited in 11/12;
- finance system - (Access Dimensions);
- GIS – ESRI Product;
- CAMS – Countryside/Navigational Access Management Systems - (Exegesis CAMS);
- HR System – (Snowdrop);
- document management – (Sharepoint); and
- asset management – currently going through a project to move from a spreadsheet based solution.

DragonFly House:

DragonFly house is a relatively new building within the City of Norwich. The facility is owned and managed by DEFRA and houses five public sector organisations 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 Authority's office areas. Although this was raised as an area of concern during the previous needs assessment process, management at the Authority have decided to accept the risk.

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, and allows IT Service support services to connect in to support IT systems. The TREO phones have now been replaced with Blackberry Devices to improve security. 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 2003/2008;
- the main Laptop and Desktop O/S is Windows 2007/XP;
- Sharepoint is Microsoft Sharepoint 2003, however, the Authority wants to move to Microsoft Office Sharepoint Server (MOSS) 2010; and
- Desktop office applications use Microsoft Office 2007/XP.

Server room and Backups:

The main building is managed by Defra Estates 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. Broads Authority staff have access to the server room for management of backup tapes.

6. 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 agree timings. As only a small part of the IT Infrastructure can be covered, it is expected that the Authority will seek internal management assurance that key risk areas are being adequately managed. Where possible, we have consolidated work to give synergy between areas to provide best value, however, the audits will be undertaken at a high scope level to provide the widest possible coverage. These audits can only be achieved in these timescales due to the size of the organisation and the localisation of the IT team. Where necessary, these audits can be split out into smaller segments of work, however, if undertaken

individually, they will require more audit time.

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

1) Network Security – 7 days – to form part of the 13/14 IT Audit Plan

a. Network Security (Domain Controller Settings)

b. Virus Protection/Spyware – (on the Domain Controller)

c. Data Backup – Dragonfly House

d. Data Centre – Dragonfly House

2) End User Controls – 7 days – to form part of the 14/15 IT Audit Plan

a. PC End User controls (and confirmation Virus Protection is installed and updated)

b. Laptop Security (and confirmation Virus Protection is installed and updated)

c. Mobile Devices (Phones/USB, etc)

d. End User Device Asset Management

3) Exchange and e-mail – 7 days – to be held in reserve

a. Exchange and e-mail

APPENDIX 1 - Computer Audit Needs Assessment Results

AUDITABLE AREA		Authority Comments	Previous Audit / Proposed Audit	Risk Area from Risk Log					
				Financial Overspend / Significant Loss of Income	Ineffective Management of Assets	Ineffective Project Management	Loss of IT / Communications Systems	Loss of Offices including Field Bases	Non Availability of Key Staff
Infrastructure									
Unauthorised network access									
Network Infrastructure	**M**	This is under contract from DEFRA and the Broads Authority has responsibility for switches and policing.					X	X	
Network Security	**H**	Internally Managed – The network is protected by Firewalls and authentication is via Active Directory.	(1)				X	X	
Wireless Networks	**L**	One access point is connected to the DMZ for meetings for visitors so is a feed to the outside world only. Although the Authority is Looking to replace hardware there is no internal network access through the wireless access point.					X	X	
Virus Protection/Spyware	**H**	This was changed a year ago ESET nod32. Since then no infections have been noted. In addition, the Authority Still uses CA gateway security which acts as a proxy server on e-mail and web services at the perimeter.	(1) - (on the Domain Controller). (2) – (on PC's and Laptops)				X		
Firewalls	**M**	These are internally managed. There are two Firewalls with IDS. Incoming ports are limited with outgoing more open and was configured through a lock down and white listing process.					X		
Virtualisation	**M**	The server farm has been virtualised with assistance from an external supplier.					X	X	
WAN	**L**	Hardware VPN's are used between remote sites of which there are a limited number.					X	X	
Unauthorised Remote user access									
Remote Access (User)	**M**	There are a number of remote users but if they could not connect they would be able to visit the office. Access is managed by certificates on the machines and password strength has been increased to 8 character complex passwords.					X	X	
Remote Access (Supplier)	**M**	Access for suppliers is blocked unless a change is required (the main systems supported in this way are Tolls and Planning). The authority is moving more to WebEx which allows the authority to observe actions being taken when the supplier is connected. If a supplier could not connect they would be able to visit the offices.					X	X	
Poor/insecure communications									
Telecoms/VoIP	**M**	There is a mix of telecoms and VOIP; if there were any issues most staff members also have mobile phones (e.g. Remote workers). The phone contract has now changed to include call charges per minute so there is greater scrutiny and the Authority is looking at increased reporting.					X	X	
Content Management (Web site (Internet))	**M**	This is externally hosted and editorial privileges are limited to one user per department. Content managed internally and then passed through to Web Manager to authorise and publish.					X	X	

AUDITABLE AREA		Authority Comments	Previous Audit / Proposed Audit	Risk Area from Risk Log					
				Financial Overspend / Significant Loss of Income	Ineffective Management of Assets	Ineffective Project Management	Loss of IT / Communications Systems	Loss of Offices including Field Bases	Non Availability of Key Staff
Content Management (Web site (Intranet))	L	Currently SharePoint and separate document libraries are used and the Web manager manages this service.					X	X	
Exchange server and e-mail	H	There is a lot of reliance placed on e-mail for storage of information and communication and currently exchange 2010 is in use.	(3)				X	X	
Internet	L	Short periods of time without internet access would have little impact on the Authority's services.					X	X	
End user equipment loss or compromise									
PC End User controls	M	PC's are restricted to office locations and as such are less vulnerable than mobile devices. All hard drives are wiped prior to the disposal of any machine.	(2)		X		X		
Laptop Security	H	There are a number of laptops in use across the Authority and by remote workers. Encryption has been included on the latest laptops, however, the older laptops are not encrypted.	(2)		X		X	X	
Mobile Devices (Phones/USB, etc) - All smart phones blackberry and can remote wipe	H	There is no port control on the Authority systems to prevent unauthorised devices (such as unencrypted USB Drives) being connected to the systems, although for smart phones there is a remote wipe facility if a device were to go missing.	(2)		X		X	X	X
Asset Management	M	A full list of IT assets is maintained by the IT Team.	(2)		X				
Management Issues									
Poor Recovery and Contingency									
Business Continuity (BS25999)	M	This has been developed and scheduled for update.					X	X	X
Disaster Recovery	M	This is in place, however, it needs updating to reflect virtualisation and the proposed extension to the dock site.	08/09				X	X	
Data Back-up	H	Failure to backup could result in lost data if there were an issue. We are currently making changes to Storage Area Network (SAN) after which the weekly tape will be kept off site at the dockyard facility.	(1)				X	X	
Data Centre	H	This is a shared facility so the Authority does not have full control over who has access.	(1)				X		
Poor IT Support									
Change control and Release Management	M	Test environments are in use before releasing changes, which has been greatly helped by Virtualisation.					X		
Helpdesk/Service Desk	M	Items are logged in SharePoint relating to problems and incidents					X		
Availability Management	L	There is a dashboard for review which also provides alerts at defined levels					X		
Capacity Management	L	Capacity is monitored					X		

AUDITABLE AREA		Authority Comments	Previous Audit / Proposed Audit	Risk Area from Risk Log					
				Financial Overspend / Significant Loss of Income	Ineffective Management of Assets	Ineffective Project Management	Loss of IT / Communications Systems	Loss of Offices including Field Bases	Non Availability of Key Staff
Configuration Management	L	Dependencies are known as this is a relatively simple system.					X		
Incident and Problem Management	M	Problems are recorded in SharePoint and a weekly meeting is held to consider trends, and any actions which need to be taken.					X		
Service level Management	L	SLA's externally but not internally as the majority of staff are based on the same floor.					X		
Support Contract Management	M	Support contracts are in place for almost all systems to some extent to provide resilience in service.					X		
Poor general understanding and control									
Policy/ ISO27001/ ITIL/ ISO9000	M	There are very few IT Policies in place - Electronic communications policy (e.g. Some personal use). New members sign the policy and established staff re-sign on an annual basis. Although the Policy is not based on ISO27001, it is based around best practice from a variety of sources.	10/11	X	X	X	X		X
Governance	M	The Authority is still small enough for IT to maintain good links with all departments and the structure has changed to accommodate this growth. We now have a corporate ICT group to highlight the issues and forthcoming projects which includes representatives from the Authority, the Chief exec and IT. The group meets twice a year and is proving to be a useful forum.	10/11	X	X	X	X		X
Procurement/ Acquisition	M	IT is bound by the procurement strategy.		X	X		X		
Authority unable to meet changing demands									
Project Management	M	We have a project manager who looks after the projects for the Authority.		X		X			
Strategy	M	A corporate ICT group now exists to highlight the issues and forthcoming projects which includes representatives from the Authority, the Chief Executive and IT. The group meets twice a year and is proving to be a useful forum and has been tasked with agreeing a three year strategic plan, although currently they only cover the following year.	10/11	X	X				X
Breach of law / financial regulations									
Software Licensing (inc FAST)	M	A licence dashboard has been procured but as yet has not been utilised to its full extent. Education area is covered until 2013 so there are enough licences to cover most people, however, and deficiencies in licences will likely be due to people loading their own software which the dashboard will help monitor.			X		X		
Data Protection	M	There is a DPA Officer.		X	X		X	X	
Freedom of Information	L	There is a freedom of information officer.		X					

AUDITABLE AREA		Authority Comments	Previous Audit / Proposed Audit	Risk Area from Risk Log					
				Financial Overspend / Significant Loss of Income	Ineffective Management of Assets	Ineffective Project Management	Loss of IT / Communications Systems	Loss of Offices including Field Bases	Non Availability of Key Staff
Applications									
Planning applications and records	**M**	The application is used for the recording of Planning applications and planning records under the Authority jurisdiction.		**X**			**X**		**X**
Vessel Registrations – includes licensing system	**M**	The application used for Vessel registrations and includes the Licensing System.	11/12	**X**			**X**		**X**
Finance system (Access Dimensions)	**M**	Finance application used for recording and managing the Authority's finances		**X**			**X**		**X**
GIS – ESRI Product	**L**	The GIS System is used to capture, store, manipulate, analyze, manage, and present all types of geographically referenced data in relation to the Broads.			**X**		**X**		**X**
CAMS – Countryside Access Management Systems	**L**	Used to monitor and maintain access (Countryside and Navigational) routes around the Broads.					**X**		**X**
HR System – Snowdrop	**M**	Is used to manage the HR requirements of the Authority.		**X**			**X**		**X**
Payroll external - Broadland	**L**	Payroll is managed by Broadland District Council.		**X**			**X**		
Document management	**H**	Document management is used to scan and store the Authority Documents in an electronic format. This received a 'high' risk rating due to the ability to more easily share and view electronic documentation than physical.					**X**	**X**	

APPENDIX 2 - Glossary of key terms

CA gateway: Anti Virus Solution

DEFRA: Defra is the UK government department responsible for policy and regulations on the environment, food and rural affairs

DMZ: DMZ (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network

ESET nod32: Anti virus solution.

IDS: An intrusion detection system (IDS) is a device or software application that monitors network and/or system activities for malicious activities or policy violations and produces reports to a Management Station.

ISO27001: ISO 27001 is the international best practise for an Information Security Management System (ISMS).

virtualisation: Virtualization (or virtualisation), in computing, is the creation of a virtual (rather than actual) version of something, such as a hardware platform, operating system, a storage device or network resources.

VOIP: Voice over IP (VoIP) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

VPN's: A virtual private network (VPN) is a network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote offices or traveling users an access to a central organizational network.

WebEx: WebEx combines desktop sharing through a web browser with phone conferencing and video and allows remote support.

Appendix C – Needs assessment timetable

	DATES
Planning Meeting	January 2012
Fieldwork Start	07 February 2012
Fieldwork completion	27 February 2012
Exit Meeting	27 February 2012
Draft report issued to client	16 March 2012 (Revised version)
Final report issued to client	23 April 2012