Audit and Risk Committee

26 July 2022
Agenda item number 8

Internal Audit annual report and opinion 2021/22

Report by Head of Internal Audit

Summary

This report provides the Authority with an Annual Report and Opinion for 2021/22, drawing upon the outcomes of Internal Audit work performed over the course of the year and a conclusion on the Effectiveness of Internal Audit.

Recommendation

The Committee is requested to:

1. Receive and approve the contents of the Annual Report and Opinion of the Head of Internal Audit.
2. Note that a reasonable audit opinion (positive) has been given in relation to the framework of governance, risk management and control for the year ended 31 March 2022.
3. Note that the opinions expressed together with significant matters arising from internal audit work and contained within this report should be given due consideration, when developing and reviewing the Authority's Annual Governance Statement for 2021/22.
4. Note the conclusions of the Review of the Effectiveness of Internal Audit.

1. Introduction/background

1.1. In line with the Public Sector Internal Audit Standards, which came into force from 1 April 2013, an annual opinion should be generated which concludes on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control:

- A summary of the work that supports the opinion should be submitted;
- Reliance placed on other assurance providers should be recognised;
- Any qualifications to that opinion, together with the reason for qualification must be provided;

- There should be disclosure of any impairments or restriction to the scope of the opinion;
- There should be a comparison of actual audit work undertaken with planned work;
- The performance of internal audit against its performance measures and targets should be summarised; and,
- Any other issues considered relevant to the Annual Governance Statement should be recorded.

1.2. This report also contains conclusions on the Review of the Effectiveness of Internal Audit, which includes;

- The degree of conformance with the PSIAS and the results of any quality assurance and improvement programme;
- The outcomes of the performance indicators; and,
- The degree of compliance with CIPFA's Statement on the Role of the Head of Internal Audit.

1.3. The Annual Report and Opinion 2021/22 and the Review of the Effectiveness of Internal Audit are shown in the report attached.

1.4. On the basis of Internal Audit work performed during 2021/22, the Head of Internal Audit is able to give a reasonable opinion (positive) on the framework of governance, risk management and control at the Broads Authority.

1.5. The outcomes of the Effectiveness Review confirm that Internal Audit:

- Is compliant with the Public Sector Internal Audit Standards;
- Is continually monitoring performance and looking for ways to improve; and.
- Is complaint with CIPFA Statement on the Role of the Head of Internal Audit in Public Service Organisations.

1.6. These findings therefore indicate that reliance can be placed on the opinions expressed by the Head of Internal Audit, which can then be used to inform the Authority's Annual Governance Statement.

Author: Faye Haywood

Date of report: 28 June 2022

Appendix 1 – BA Annual report and opinion 2021/22

Eastern Internal Audit Services

BROADS AUTHORITY

Annual Report and Opinion 2021/22

Responsible Officer: Faye Haywood – Head of Internal for Broads Authority

CONTENTS

1. INTRODUCTION

1.1 The Accounts and Audit Regulations 2015 require that "a relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account public sector internal auditing standards or guidance".

1.2 Those standards – the Public Sector Internal Audit Standards - require the Chief Audit Executive to provide a written report to those charged with governance (known in this context as the Audit and Risk Committee) to support the Annual Governance Statement (AGS). This report must set out:

- The opinion on the overall adequacy and effectiveness of the Authority's framework of governance, risk management and control during 2021/22, together with reasons if the opinion is unfavourable;
- A summary of the internal audit work carried from which the opinion is derived, the follow up of management action taken to ensure implementation of agreed action as at financial year end and any reliance placed upon third party assurances;
- Any issues that are deemed particularly relevant to the Annual Governance Statement (AGS);
- The Annual Review of the Effectiveness of Internal Audit, which includes; the level of compliance with the PSIAS and the results of any quality assurance and improvement programme, the outcomes of the performance indicators and the degree of compliance with CIPFA's Statement on the Role of the Head of Internal Audit.

1.3 When considering this report, the statements made therein should be viewed as key items which need to be used to inform the organisation's Annual Governance Statement, but there are also a number of other important sources to which the Audit and Risk Committee and statutory officers of the Authority should be looking to gain assurance. Moreover, in the course of developing overarching audit opinions for the authority, it should be noted that the assurances provided here, can never be absolute and therefore, only reasonable assurance can be provided that there are no major weaknesses in the processes subject to internal audit review. The annual opinion is thus subject to inherent limitations (covering both the control environment and the assurance over controls) and these are examined more fully at **Appendix 5**.

2. ANNUAL OPINION OF THE HEAD OF INTERNAL AUDIT

2.1 Roles and responsibilities

- The Authority is responsible for establishing and maintaining appropriate risk management processes, control systems, accounting records and governance arrangements.
- The AGS is an annual statement by the Chairman of the Authority and the Chief Executive that records and publishes the Authority's governance arrangements.
- An annual opinion is required on the overall adequacy and effectiveness of the Authority's framework of governance, risk management and control, based upon and limited to the audit work performed during the year.

This is achieved through the delivery of the risk based Annual Internal Audit Plan discussed and approved with Management Team and key stakeholders and then approved by the Audit and Risk Committee at its meeting on 2 March 2021.

This opinion does not imply that internal audit has reviewed all risks and assurances, but it is one component to be taken into account during the preparation of the AGS.

The Audit and Risk Committee should consider this opinion, together with any assurances from management, its own knowledge of the Authority and any assurances received throughout the year from other review bodies such as the external auditor.

2.2 The opinion itself

The overall opinion in relation to the framework of governance, risk management and controls at the Broads Authority is **reasonable**, with all four audits concluding with a positive assurance grading in Key Controls and Assurance, Cyber Security, Corporate Governance Risk Management and HR & Payroll.

The audit of Key Controls and Assurance resulted in a substantial assurance.

No urgent priority findings have been raised at the Authority for 2021/22. It is for that reason it is felt that a reasonable assurance opinion overall applies.

In providing the opinion, the authority's risk management framework and supporting processes, the relative materiality of the issues arising from the internal audit work during the year and management's progress in addressing any control weaknesses identified therefrom have been taken into account.

The opinion has been discussed with the Section 17 Officer prior to publication.

3. AUDIT WORK UNDERTAKEN DURING THE YEAR

3.1 **Appendix 1** records the internal audit work delivered during the year on which the opinion is based. In addition, **Appendix 2** is attached which shows the individual assurances provided over recent financial years to provide an overall picture of the control environment.

3.2 Summary of internal audit work

The Audit and Risk Committee approved the Annual Internal Audit Plan for 2021/22, which is summarised at **Appendix 1** to this report and totalled 36 days as originally planned, encompassing:

- An annual opinion of Corporate Governance and Risk Management;
- A fundamental financial system review of key controls and assurance, including verification of completion of audit recommendations;
- HR & Payroll;
- Cyber Security.

A total of 17 recommendations were raised in 2021/22.

3.3 At **Appendix 3** to this report a detailed Executive Summary is provided for each 2021/22 audit undertaken. The Cyber Security Maturity Assessment report is currently in draft, the overall opinion for this work has been considered in the formulation of this opinion. Management are currently considering the recommendations.

3.4 Follow up of management action

In relation to the follow up of management actions the position at year end is that of the 11 recommendations raised and agreed by TIAA Ltd in 2021/22, four are complete; one important recommendation is outstanding; and four are within deadline. Two risk management recommendations have been rejected by management.

3.4.1 A total of one needs attention recommendation remains overdue from 2019/20 Procurement audit; two important recommendations are overdue from the 2020/21 Port Marine Safety Code audit, and one needs attention recommendation is overdue from the 2020/21 Corporate Governance and Risk Management audit. A summary showing progress against the implementation of agreed internal audit recommendations can be found at **Appendix 4.**

3.5 Issues for inclusion in the Annual Governance Statement

Internal Audit work has not identified any weaknesses that are significant enough for disclosure within the Annual Governance Statement.

4. THIRD PARTY ASSURANCES

4.1 In arriving at the overall opinion reliance has not been placed on any third-party assurances.

5. ANNUAL REVIEW OF THE EFFECTIVENESS OF INTERNAL AUDIT

5.1 Quality Assurance and Improvement Programme (QAIP)

5.1.1 Internal Assessment

A checklist for conformance with the PSIAS and the Local Government Application Note has been completed for 2021/22. This covers; the Definition of Internal Auditing, the Code of Ethics and the Standards themselves.

The Attribute Standards address the characteristics of organisations and parties performing Internal Audit activities, in particular; Purpose, Authority and Responsibility, Independence and Objectivity, Proficiency and Due Professional Care, and Quality Assurance and Improvement Programme (which includes both internal and external assessment).

The Performance Standards describe the nature of Internal Audit activities and provide quality criteria against which the performance of these services can be evaluated, in particular; Managing the Internal Audit Activity, Nature of Work, Engagement Planning, Performing the Engagement, Communicating Results, Monitoring Progress and Communicating the Acceptance of Risks. On conclusion of completion of the checklist full conformance has been ascertained in relation to the Definition of Internal Auditing, the Code of Ethics and the Performance Standards.

The detailed internal assessment checklist is provided to the Director of Finance for independent scrutiny and verification.

5.1.2 External Assessment

In relation to the Attribute Standards it is recognised that to achieve full conformance an external assessment is needed. This is required to be completed every five years, with the first review having been completed in January 2017.

The external assessment was undertaken by the Institute of Internal Auditors concluded that "**the internal audit service conforms to the professional standards and the work has been performed in accordance with the International Professional Practices Framework**".

The next assessment is due for October 2022. The results of this will be provided to the Committee.

5.2 Performance Indicator outcomes

5.2.1 The Internal Audit Service is benchmarked against a number of performance measures. Actual performance against these targets is outlined in the following table:

Area / Indicator	Frequency	Target	Actual	Comments
Audit Committee / Senior Management				
1. Audit Committee Satisfaction – measured annually	Annual	Adequate	N/A	New committee Chair
2. Director of Finance Satisfaction – measured quarterly	Annual	Good	Good	Achieved
Internal Audit Process				
3. Each quarter's audit's completed to draft report within 10 working days of the end of the quarter	Quarterly	100%	50%	Not achieved, 2 reports issued within 10 working days of quarter end.
4. Quarterly assurance reports to the Contract Manager within 15 working days of the end of each quarter	Quarterly	100%	0%	Not achieved.
5. An audit file supporting each review and showing clear evidence of quality control review shall be completed prior to the issue of the draft report (a sample of these will be subject to quality review by the Contract Manager)		100%	100%	Achieved
6. Compliance with Public Sector Internal Audit Standards		Generally conforms	Generally conforms	Achieved
7. Respond to the Contract Manager within 3 working days where unsatisfactory feedback has been received.		100%	n/a	No unsatisfactory feedback received.
Clients				
8. Average feedback score received from key clients (auditees)		Adequate	Good	Exceeded
9. Percentage of recommendations accepted by management		90%	88%	Not achieved; 2 out of 17 recommendations raised rejected
Innovations and Capabilities				
10. Percentage of qualified (including experienced) staff working on the contract each quarter		60%	75%	Exceeded
11. Number of training hours per member of staff completed per quarter		1 day	1 day	Achieved

5.2.2 Performance has not been in line within the boundaries of our agreed targets in some areas during 2021/22 such as the issuing of draft reports 10 day after quarter end, performance reports being provided within a 15 working day window after quarter end and percentage of recommendations accepted by management.

As reported to the Audit and Risk Committee throughout the year, Internal Audit performance has continued to be impacted in 2021/22 by the Covid-19 pandemic. A period of adjustment was also required in response to prolonged remote working practices. Contractor resourcing and sickness were also a key challenge throughout the year.

This performance result has been experienced across the internal audit consortium in 2021/22 with other third-party assurance providers also reporting similar challenges. Resourcing levels did settle in time to ensure the 2021/22 plan of work could be completed.

In response to the challenges faced this year, the Head of Internal Audit has enhanced communication and monitoring arrangements. The contractor has also committed to reviewing resource planning processes by allocating resources and booking in audits well in advance of the proposed start date.

The 2021/22 procurement exercise has now concluded which will see the current contractor continue to provide the Internal Audit service. The Head of Internal Audit has used this opportunity strengthen the key performance measures around timeliness included within the contract.

5.3 Effectiveness of the Head of Internal Audit (HIA) arrangements as measured against the CIPFA Role of the HIA

5.3.1 This Statement sets out the five principles that define the core activities and behaviours that apply to the role of the Head of Internal Audit, and the organisational arrangements to support them. The Principles are:

- Champion best practice in governance, objectively assessing the adequacy of governance and management of risks;
- Give an objective and evidence based opinion on all aspects of governance, risk management and internal control;
- Undertake regular and open engagement across the Authority, particularly with the Management Team and the Audit and Risk Committee;
- Lead and direct an Internal Audit Service that is resourced to be fit for purpose; and
- Head of Internal Audit to be professionally qualified and suitably experienced.

5.3.2 Completion of the checklist confirms full compliance with the CIPFA guidance on the Role of the Head of Internal Audit. The detailed checklist has been forwarded to the Director of Finance for independent scrutiny and verification.

APPENDIX 1 – AUDIT WORK UNDERTAKEN DURING 2021/22

Audit Area	**Assurance**	**No of Recs**	**Implemented**	**P1 OS**	**P2 OS**	**P3 OS**	**Not yet due**
Annual Opinion Audits							
Corporate Governance and Risk Management	Reasonable	6	4	0	0	0	2
Fundamental Financial Systems							
Key Controls and Assurance	Substantial	1	0	0	0	0	1
Service area audits							
HR & Payroll	Reasonable	4	2	0	1	0	1
Cyber Security	Reasonable (DRAFT)	6	0	0	0	0	6
Total		**17**	**6**	**0**	**1**	**0**	**10**

Assurance level definitions		Number
Substantial Assurance	Based upon the issues identified there is a robust series of suitably designed controls in place upon which the organisation relies to manage the risks to the continuous and effective achievement of the objectives of the process, and which at the time of our audit review were being consistently applied.	1
Reasonable Assurance	Based upon the issues identified there is a series of internal controls in place, however these could be strengthened to facilitate the organisations management of risks to the continuous and effective achievement of the objectives of the process. Improvements are required to enhance the controls to mitigate these risks.	3
Limited Assurance	Based upon the issues identified the controls in place are insufficient to ensure that the organisation can rely upon them to manage the risks to the continuous and effective achievement of the objectives of the process. Significant improvements are required to improve the adequacy and effectiveness of the controls to mitigate these risks.	0
No Assurance	Based upon the issues identified there is a fundamental breakdown or absence of core internal controls such that the organisation cannot rely upon them to manage risk to the continuous and effective achievement of the objectives of the process. Immediate action is required to improve the controls required to mitigate these risks.	0

Urgent – Priority 1	Fundamental control issue on which action to implement should be taken within 1 month.
Important Priority 2	Control issue on which action to implement should be taken within 3 months.
Needs Attention – Priority 3	Control issue on which action to implement should be taken within 6 months.

APPENDIX 2 ASSURANCE CHART

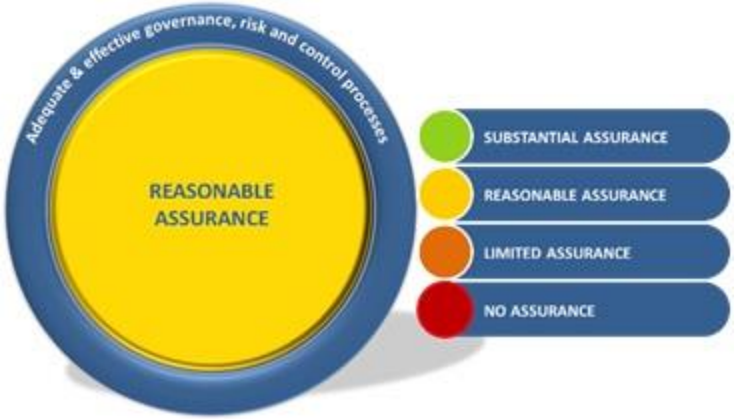
	2018-19	2019-20	2020-21	2021-22	2022-23
Annual Opinion Audits					
Corporate Governance and Risk Management	Reasonable	Reasonable	Reasonable	Reasonable	X
Fundamental Financial Systems					
Key Controls and Assurance Work	Substantial	Substantial	Reasonable	Substantial	X
HR and Payroll				Reasonable	
Procurement		Reasonable			
Services Area Reviews					
External Funding - HLF Bid and National Parks Partnership		Reasonable			
Asset Management					
Port Marine Safety Code			Limited		
Branding	Reasonable				
Planning			Reasonable		
Corporate Health and Safety					X
Partnership Working					X
IT Audits					
Toll Management Application					
Network Security					
Cyber Security				Reasonable	
End User Controls					
Disaster Recovery	Reasonable				
Virus Protection/Spyware, Data Backup and Data Centre controls					

APPENDIX 3 – EXECUTIVE SUMMARIES

Assurance Review of BA2201 Corporate Governance and Risk Management

Executive Summary

OVERALL ASSURANCE ASSESSMENT



ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Governance arrangements for decision making	0	0	1	0
Performance Monitoring	0	0	0	0
Risk Management Framework	0	1	4	0
Total	**0**	**1**	**5**	**0**

SCOPE

Our annual review of governance and risk management was carried out to support the Head of Internal Audit Opinion. This audit provides assurance that the systems in place to control and manage the Broads Authority are operating effectively and that significant risks are being identified and managed. During our review we considered governance arrangements for decision making and the accountability and monitoring of performance during the Covid-19 Pandemic. Our review also provides assurance over the Risk Management framework to give a view as to whether it has supported the achievement of strategic priorities.

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Reasonable Assurance' in managing the risks associated with the audit. The assurance opinion has been derived as a result of one ‘Important’ and five 'needs attention' recommendations being raised upon the conclusion of our work.
- The previous audit of Corporate Governance and Risk Management also concluded in a ‘Reasonable’ assurance opinion, having raised two ‘important’ and five ‘needs attention’ recommendations. This indicates a positive direction of travel.

POSITIVE FINDINGS

It is acknowledged there are areas where sound controls are in place and operating consistently:

Governance arrangements for decision making

- A review of Committees and a sample of decisions confirmed that Standing Orders and Terms of Reference have been complied with.
- Actions taken where Members have a conflict of interest are logged and recorded within Appendix 1 of the Authority's or Sub-Committee's minutes.
- The Authority has an up-to-date Members Code of Conduct. Members are required to sign and return an undertaking in respect of the Code. A sample check found this process to be in place.

Performance Monitoring

- An annual business plan is published on the Authority's website containing the strategic priorities of the Authority. This underpins the 2017-2022 Broads Plan, and clearly highlights the priorities in which the Broads Authority is lead partner for. This helps demonstrate part of the 'golden thread' i.e. how the performance of the strategic priorities are aligned to the main corporate plan of the Authority.
- Progress on the strategic priorities within the Broads Plan are reported to each Broads Authority and published on the website.

Risk Management Framework

- The Risk Management Policy has been recently reviewed, updated and endorsed by the Audit and Risk Committee.
- The Policy provides details of how risks are to be identified at strategic and operational level, and how they are to be assessed.
- There are currently ten risks on the Corporate Risk Register. This is a manageable number of risks. All risks are reviewed in line with the Risk Management Policy and Committee and management meeting schedules.

ISSUES TO BE ADDRESSED

The audit has highlighted the following area where one ‘important’ recommendation has been made.

Risk Management Framework

- The risks within the Corporate and Directorate Risk Registers be linked to the organisation’s objectives.

The audit has also highlighted the following areas where five 'needs attention' recommendations have been made.

Governance arrangements for decision making

- All Members' Declarations of Interest forms be checked to ensure that they have been fully completed, returning any with blank fields to the relevant Member for completion.

Risk Management Framework

- A review be undertaken of those risks within the Corporate Risk Register with scores under 16 to ensure they comply with the Risk Management Policy.
- Management to include a target risk score within the risk registers.
- Management to undertake a Training Needs Assessment in respect of Risk Management and introduce Risk Management training if deemed necessary.
- Management to instigate using a spreadsheet instead of a word document for the risk registers so that a formula can be used for the risk assessment and RAG rating.

Operational Effectiveness Matters

There are no operational effectiveness matters for management to consider.

Previous audit recommendations

The previous report was issued in March 2021 (BA/21/04), with a ‘Reasonable’ assurance, having raised one ‘important’ and three ‘needs attention’ recommendations. These have all been completed with the exception of one ‘needs attention’ recommendation (Recommendation 2), which refers to the update and review of the document management system (DMS), a revised date of December 2022 being provided.

Other points noted

- The audit has concluded with the following two disagreed recommendations:

  Management to include a target risk score within the risk registers.

  Management response - Management Team agreed on 26.04.22 that they did not consider this necessary as the aim was always to have as low as possible risk score, through the appropriate mitigation.

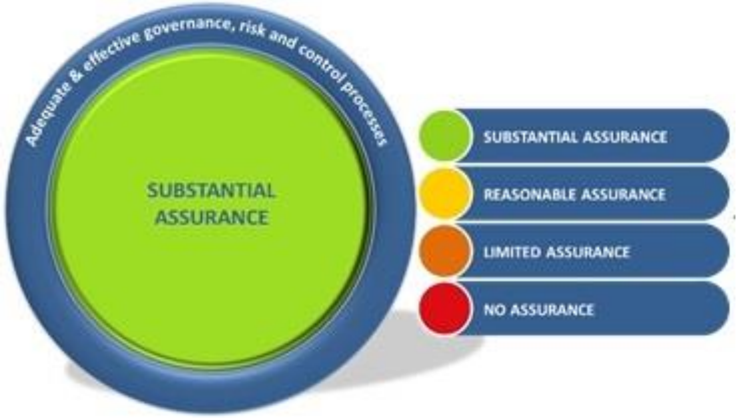
  Management to instigate using a spreadsheet instead of a word document for the risk registers so that a formula can be used for the risk assessment and RAG rating.

  Management response: Management Team agreed on 26.04.22 to maintain the use of a Word document as this was their preference. Suitable measures were in place to check the risk rating and colour coding were aligned.

Assurance Review of BA2202 Key Controls and Assurance Framework

Executive Summary

OVERALL ASSURANCE ASSESSMENT



ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Treasury Management	0	0	1	0
General Ledger	0	0	0	0
Asset Management	0	0	0	0
Accounts Payable	0	0	0	0
Toll Income	0	0	0	0
Total	0	0	1	0

No recommendations were also raised in relation to accounts receivable, budgetary control or control accounts.

SCOPE

This audit looked at the fundamental systems that feed into the statement of accounts to provide assurance on the key financial controls. The areas reviewed as part of this audit were; Treasury Management/Investments, General Ledger, Asset Management, Budgetary Control, Accounts Receivable, Accounts Payable, Toll Income, Control Accounts, and Follow Up of Internal Audit Recommendations.

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Substantial Assurance' in managing the risks associated with the audit. The assurance opinion has been derived as a result of one 'needs attention' recommendation being raised upon the conclusion of our work.
- The previous audit report for Key Controls (BA/21/01) was issued in May 2021. It concluded in a ‘Reasonable Assurance’ opinion with five ‘needs attention’ recommendation being raised. This indicates a positive direction of travel.

POSITIVE FINDINGS

It is acknowledged there are areas where sound controls are in place and operating consistently:

- Approval controls at Level 1 (L1) and Level 2 (L2) are built into the Document Management System (DMS) and invoices are not paid until L2 approval has been granted, demonstrating clear segregation of duties.
- Strong controls were evidenced with regard to BACS payment runs with a clear audit trail in place to evidence appropriate sign off in line with the documented authorised signatory list. This included the approval of cheque payments.
- Account, Investment and Fixed Asset reconciliations were found to have been appropriately signed as prepared and independently approved, demonstrating clear segregation of duties.
- The Authority provided clear evidence of budgetary control and monitoring. All variances exceeding £5k are to be explained by the budget holder and documentation was provided to support this requirement, ensuring a clear audit trail of material changes to the budget.
- Journals were raised on the system based on appropriate documentation and it was confirmed in all cases examined that journals were signed off as prepared and independently checked and approved, indicating that clear segregation of duties are in place.
- Toll Income Reconciliations, Batches, and Payments were shown to be completed and controls were in place. Appropriate action was evidenced on overdue toll payments when required, verifying that appropriate monitoring and action is taken as necessary

ISSUES TO BE ADDRESSED

The audit has also highlighted the following areas where one 'needs attention' recommendation has been made.

Treasury Management

- The Authority should consider diversifying its investment portfolio across different banking institutions**.**

Operational Effectiveness Matters

There are no operational effectiveness matters for management to consider.

Previous audit recommendations

The audit reviewed the previous internal audit recommendations, of which none remain outstanding.

Other points noted

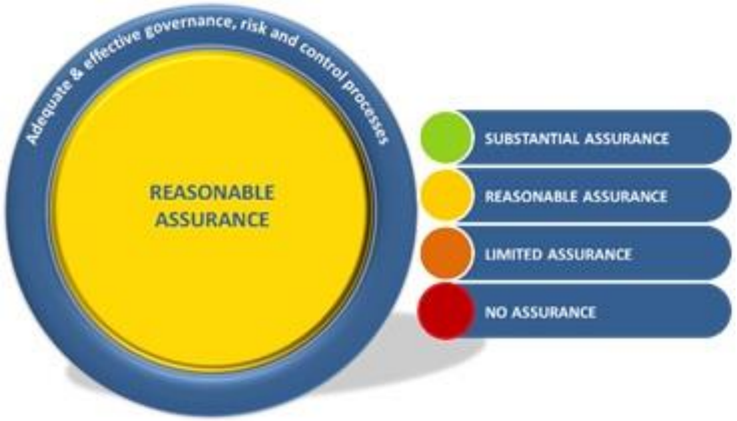
The Authority has two PWLB loans one for £290,000 taken out in 2007 and one for £105,000 taken out in November 2020. It should be noted that the loan application for 2007 could not be obtained at the point of audit fieldwork as it has been archived, therefore no formal recommendation was raised. The Authority provided evidence of the 2020 loan application, which was confirmed to have been executed by the Director of Finance in line with the Scheme of Delegation.

Overall responsibility for the Key Controls process sits with the Director of Finance who is assisted by the Financial Accountant. Discussions with the Director of Finance confirmed that the Senior Financial Officer left and there has been staffing issues. However, a new Senior Financial Officer started in January 2022, and it was advised that a new Finance Assistant is due to start at the end of January 2022 and this will bring staffing levels back up to a full complement.

Assurance Review of BA2203 HR and Payroll

Executive Summary

OVERALL ASSURANCE ASSESSMENT



ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Policies and procedures	0	0	1	0
Staff absence	0	3	0	0
HR System	0	0	0	1
Total	**0**	**3**	**1**	**1**

No recommendations have been raised in respect of Payroll Key Controls.

SCOPE

A high risk is being monitored in the Corporate Risk Register in relation to the loss of key staff. This risk has become particularly prevalent during the Covid-19 Pandemic. Our review aimed to provide assurance that staff sickness is being well managed through staff resilience plans and to ensure key services continue if sickness increases. Our review examined the robustness of Payroll processes and the implementation of the new HR software.

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Reasonable' in managing the risks associated with the audit. The assurance opinion has been derived as a result of three 'important' and one 'needs attention' recommendations being raised upon the conclusion of our work.
- The audit has also raised one 'operational effectiveness matter', which sets out matters identified during the assignment where there may be opportunities for service enhancements to be made to increase both the operational efficiency and enhance the delivery of value for money services.

POSITIVE FINDINGS

It is acknowledged there are areas where sound controls are in place and operating consistently:

- The introduction of the iTrent system has met the objectives and has reduced the administrative burden on the HR and Payroll team.
- Detailed payroll checks, including differences from the previous month, are undertaken prior to payments being made, to ensure that all payments are correct.
- All payroll payments are reviewed by the Head of HR and Financial Accountant, and authorised by the Director of Finance, to ensure segregation of duties in the process.
- All claims for additional payments are submitted and authorised through iTrent.
- Loss of key staff knowledge and expertise' has been recorded as a risk in the Corporate Risk Register and mitigating actions put in place, to ensure that there is sufficient awareness and action in respect of this risk.

ISSUES TO BE ADDRESSED

The audit has highlighted the following areas where three 'important' recommendations have been made.

Staff absence

- Resilience plans be reviewed, to ensure that they are fit for purpose and used consistently across the Authority.
- The Business Continuity Plan be reviewed and updated, to reduce the risk that staff loss or other business continuity events cause preventable service disruption.
- Absence levels be reported to senior management on a regular basis, to reduce the risk of trends and issues not being identified.

The audit has also highlighted the following areas where one 'needs attention' recommendations have been made.

Policies and procedures

- HR policies be reviewed and updated, to reduce the risk of staff being provided with outdated advice and information.

Operational Effectiveness Matters

The operational effectiveness matters, for management to consider relate to the following:

- Consideration be given to purchasing the reporting module for iTrent, to enable more effective and efficient reporting of HR data.

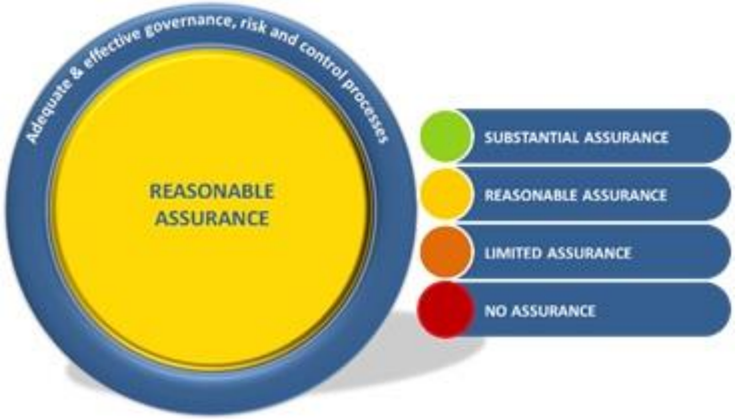
Previous audit recommendations

This area has not been subject to previous internal audit review by TIAA. Payroll key controls are reviewed as part of the annual Key Controls audit, but there are no outstanding recommendations in this area.

BA2204 Maturity Assessment of Cyber Security

Executive Summary

OVERALL ASSURANCE ASSESSMENT



ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Data Security	0	0	2	0
Incident Management	0	2	2	0
Total	**0**	**2**	**4**	**0**

No recommendations were raised in the areas of Cyber Risk Management, Engagement and Training, Asset Management, Architecture and Configuration, Vulnerability Management, Identity and Access Management, Logging and Monitoring and Supply Chain Security

SCOPE

This maturity assessment has focussed on the National Cyber Security Centre's revised 10 steps to Cyber Security framework that covers Cyber Risk Management, Engagement and Training, Asset Management, Architecture and Configuration, Vulnerability Management, Identity and Access Management, Data Security, Logging and Monitoring, Incident Management and Supply Chain Security.

Introduction

1. Organisations are facing an increasing risk of Cyber incidents and Cyber-crime. A key step to reducing the risk and protecting organisations in this area is understanding the maturity of your organisation in terms of how Cyber risks are managed. The data within this report is derived from supporting management with a self-assessment of their maturity in the following 10 recognised areas of Cyber Security:

• Cyber Risk Management	• Identity and Access Management
• Engagement and Training	• Data Security
• Asset Management	• Logging and Monitoring
• Architecture and Configuration	• Incident Management
• Vulnerability Management	• Supply Chain Security

2. The Cyber Security world is in need of a mature approach to managing cyber risk, because attackers continue to develop new threats beyond current knowledge. The fact that emerging threats are increasing is driving organisations to adopt a predictive attitude to address these threats. In order to protect themselves all organisations information assets and ICT systems need to be secured, managed and monitored.

3. Levels of recorded Cybercrime continue to grow. The Telephone-operated Crime Survey for England and Wales (TCSEW) showed that there were 1.9 million computer misuse offences in the year ending September 2021. This was an 89% increase compared with the year ending September 2019, largely driven by a 161% increase in “Unauthorised access to personal information (including hacking)” offences. This reinforces the need for users to implement robust e-Safety, including passwords based on “Three things” and not re-using the same password within multiple IT systems or websites. The National Cyber Security Centre (NCSC) provides guidance for sectors, and for users to help address the gap between good security and dangerous practices.

4. The Covid-19 Pandemic has also been instrumental in increasing risks associated with Cyber Crime. Many attacks are thematic in nature and continue to exploit users’ interest in the latest pandemic news including around access to vaccinations. Coupled with a rapid IT transformation to enable home working with new IT systems and products, the associated likelihood of cybercrimes manifesting has also increased.

5. The potential impact from cybercrime can be of substantial damage to the operational capability of the organisation. Legislative impact is within the scope of the Data Protection Act 2018, which embodies the General Data Protection Regulations (GDPR). It requires data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage. This places a requirement on all organisations to ensure that appropriate technical and organisational measures are in place. The potential level of fines for Data Protection breaches (including as a result of hacking) are up to 20m Euros / £18m or 4% of global annual turnover whichever is the greater. In addition to the financial penalties, breaches cause significant reputational damage to affected organisations, including those using cloud based IT services.

6. In assessing maturity, the current maturity level for each of the 10 areas has been identified and management’s aspirations and appetite for improvement to manage and mitigate risk have been ascertained. This work was carried out in February and March 2022 by the Cyber Assurance team as part of the proactive Internal Audit programme for 2021/22. Note that the audited maturity levels shown reflect an acknowledgement of the reduced level of data risk that the Authority is exposed to. Hence, the audited maturity levels are higher than they might have been if the existing controls infrastructure in place here were to be applied to another larger and more complex organisation that holds large quantities of Personal Identifiable Data. Such organisations require a greater level of risk mitigation due to the data that those organisations process.

7. TIAA's Cyber Maturity model is based on the traditional maturity model, and comprises of levels 0-5 as described below:

Level	Status	Description
0	Incomplete	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
1	Initial	Unpredictable process that is poorly controlled and reactive
2	Managed	Process is planned, documented and monitored ad-hoc and is often reactive
3	Defined	Proactive process meant for organizations
4	Quantitative	Measured and controlled process
5	Optimising	Focus is on continuous process and improvement

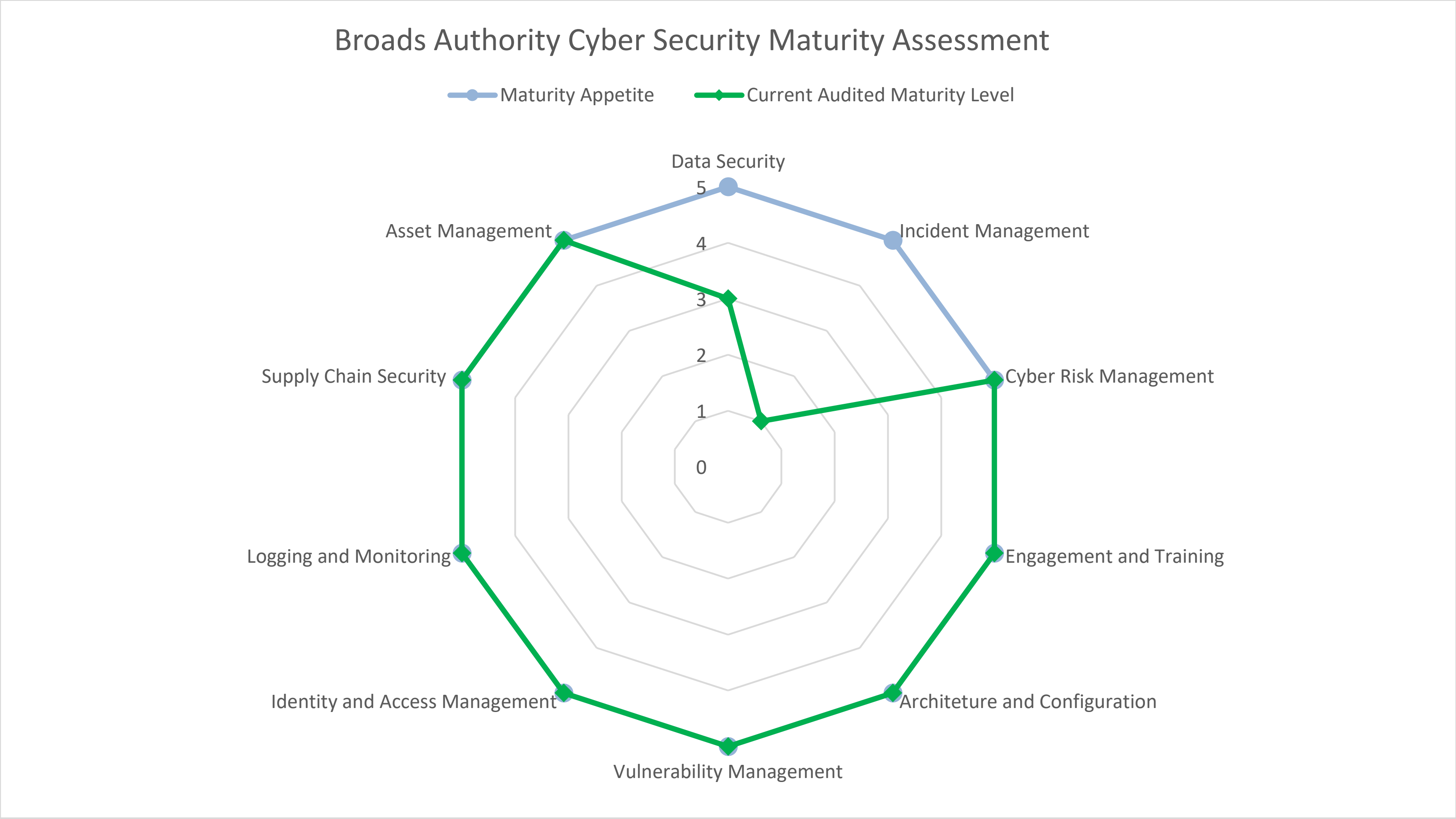
Summary

8. The review noted that management rated the Broads Authority's dependency on Information technology as high and recognised that Cyber-crime is a significant risk. Management considered that untreated cyber risks were at a medium level. It was noted that the Authority had invested in improving cyber security measures in the last 12 months.

9. The Authority has not experienced any cyber incidents within the last 12 months.

10. TIAA's maturity assessment is summarised in the radar diagram below. Significant gaps or 2 or more maturity steps exist between the aspirational level of maturity and the assessed level for the following process areas: Data Security and Incident Management.

11. Where gaps have been identified management should consider TIAA's maturity improvement recommendations within this report (summarised at Appendix A) to further control and mitigate cyber risks.


Broads Authority Cyber Security Maturity Assessment
Maturity Appetite
Current Audited Maturity Level
Data Security
Incident Management
Cyber Risk Management
Engagement and Training
Architeture and Configuration
Vulnerability Management
Identity and Access Management
Logging and Monitoring
Supply Chain Security
Asset Management
5
4
3
2
1
0

Rec.	Cyber Area	Finding	Recommendation	To Achieve Maturity Level
DS 4	Data Security (Needs Attention)	Level 4 maturity is not fully achieved.	Backup integrity and recovery testing must take place annually to ensure that they can be recovered as expected during an incident. We note that there are occasional file restores on request from users. However, this cannot constitute adequate full testing as required by this level.	4
DS 5	Data Security (Needs Attention)	Level 5 maturity is not fully achieved.	Results of backup testing must be used to inform and improve the process via lessons learned sessions.	5
IM 2	Incident Management (Important)	Level 2 maturity is not fully achieved.	A formal IT incident management process must be established, including triage and escalation requirements. We have noted that this is in place, but that it requires review, having been last reviewed in January 2019 prior to the start of the COVID-19 pandemic	2
IM 3	Incident Management (Important)	Level 3 maturity is not fully achieved.	To achieve level IM3, full compliance with IM2 is required. In addition, IT staff must have a level of incident management training provided or disaster recovery/ business continuity exercises must be undertaken regularly. We note that this level would have been compliant in its own right had the scoring not required it to be marked as partial.	3
IM 4	Incident Management (Needs Attention)	Level 4 maturity is not fully achieved.	To achieve level IM4, full compliance with IM2 and IM3 is required. In addition, incidents must be reported and presented to senior leadership. We note that this level would have been compliant in its own right had the scoring not required it to be marked as partial.	4
IM 5	Incident Management (Needs Attention	Level 5 maturity is not fully achieved.	To achieve level IM5, full compliance with IM2, IM3 and IM4 is required. In addition, incidents must include a review and 'lessons learned' sessions, as to improve the future response. We note that this level would have been compliant in its own right had the scoring not required it to be marked as partial.	5

APPENDIX 4 – AUDIT RECOMMENDATIONS

			Completed bt 1 April 2021 to 31 March 2022			Outstanding			Total	Not yet due for implementation		
Audit Ref	**Audit Area**	**Assurance Level**	**Priority 1**	**Priority 2**	**Priority 3**	**Priority 1**	**Priority 2**	**Priority 3**	**Outstanding**	**Priority 1**	**Priority 2**	**Priority 3**
2018/19 Internal Audit Reviews												
BA1903	Branding	Reasonable			2				0			
2019/20 Internal Audit Reviews												
BA2003	Procurement	Reasonable						1	1			
2020/21 Internal Audit Reviews												
BA2101	Key Controls and Assurance	Reasonable			3				0			
BA2102	Port Marine Safety Code	Reasonable		1	5		2		2			
BA2104	Corporate Governance and Risk Management	Reasonable						1	1			
2021/22 Internal Audit Reviews												
BA2201	Corporate Governance and Risk Management				4				0		1	1
BA2202	Key Controls and Assurance								0			1
BA2203	HR and Payroll			2			1		1			1
TOTALS			**0**	**3**	**14**	**0**	**3**	**2**	**5**	**0**	**1**	**3**

Audit Title	Recommendation	Priority	Responsible Officer	Due Date	Revised Due Date	Status	Latest Response
BA2003 Procurement	Procurement training is provided to all relevant members of staff, and Members, where applicable.	3	Director of Finance	31/03/2020	30/09/2022	Outstanding	The team have been short staffed, and therefore this has not yet been completed. Now that the team are fully staffed, this recommendation is expected to be completed by 30th September 2022.
BA2102 Port Marine Safety Code	Recommendation 5: The PMSC Performance Indicators (PIs) published within the authority's PMSC and those published on the authority's website be reviewed to ensure they are consistent with each other and reflect all areas of the PMSC. The website should also be updated to reflect the latest annual PI outturns.	2	Head of Safety Management	31/10/2021	31/01/2023	Outstanding	The PI's on the website are dated 2017/2018 – The PI's reflect the Broads Plan and needs to be incorporated into the new version of the SMS. This action is a work in progress, a meeting was arranged on 21/06/22 with Director of Operations, Head of Operations & Head of Navigation to discuss the action plan in drafting new SMS version to reflect recent changes to our SMS, with implementation by January 2023.
BA2102 Port Marine Safety Code	Recommendation 9: A briefing paper to be provided to Navigation Committee outlining requirements for a legal review to ascertain if a General Direction is required for larger vessels.	2	Head of Safety Management	31/10/2021	28/02/2023	Outstanding	This recommendation requires legal input. The Risk posed by this is low as this 'Special Direction' refers to very large vessel (commercial) accessing our waters and we have not needed to use the Special Direction for many years. Due to a high demand on the navigation and other higher priority safety requirements (additional patrolling, recruiting additional Seasonal Rangers, higher prosecutions and increased visitors on the waters) this recommendation has been deferred into 2022/23 deliver year and will be progressed with our Navigation Legal expert at NPLaw. Delivery expected by Feb 2023.
BA2104 Corporate Governance and Risk Management	Recommendation 2: In relation to the document management system (DMS), the following is undertaken: Notes are added to deferred items to explain which committee date the item has been deferred to; and to review if there is a way to match up/link the items on the forward plan to the generated items area.	3	Senior Governance Officer	31/07/2021	31/12/2022	Outstanding	Governance team liaising with IT on whether more metadata can be added to improve the link between items in the Forward Plan and in the confirmed (generated report) area - progress on hold as reliant on IT resource availability, which is currently focussed on more urgent work.

Audit Title	Recommendation	Priority	Responsible Officer	Due Date	Revised Due Date	Status	Latest Response
BA2203 HR and Payroll	Recommendation 1: Staff resilience plans be reviewed to ensure that they are being used consistently across the organisation and that the activities are sufficient and effective when they have been used in practice	2	Directors	31/03/2022	30/09/2022	Outstanding	This has not yet been completed by all directorates, so it is proposed to amend the new due date to 30th September 2022.

APPENDIX 5 – LIMITATIONS AND RESPONSIBILITIES

Limitations inherent to the Internal Auditor’s work

The Internal Audit Annual Report has been prepared and TIAA Ltd (the Internal Audit Services contractor) were engaged to undertake the agreed programme of work as approved by management and the Audit and Risk Committee, subject to the limitations outlined below.

Opinions

The opinions expressed are based solely on the work undertaken in delivering the approved 2020/21 Annual Internal Audit Plan. The work addressed the risks and control objectives agreed for each individual planned assignment as set out in the corresponding audit briefs and reports.

Internal Control

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. Internal control systems essentially rely on an ongoing process of identifying and prioritising the risks to the achievement of the organisation’s policies, aims and objectives, evaluating the likelihood of those risks being realised and the impact should they be realised, and to manage them efficiently, effectively and economically. That said, internal control systems, no matter how well they have been constructed and operated, are affected by inherent limitations. These include the possibility of poor judgement in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Future Periods

Internal Audit’s assessment of controls relating to the Broads Authority is for the year ended 31 March 2022. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other matters; or,
- The degree of compliance with policies and procedures may deteriorate.

Responsibilities of Management and Internal Auditors

It is management’s responsibility to develop and maintain sound systems of risk management, internal control and governance and for the prevention and detection of irregularities and fraud. Internal Audit work should not be seen as a substitute for management’s responsibilities for the design and operation of these systems.

The Head of Internal Audit has sought to plan Internal Audit work, so that there is a reasonable expectation of detecting significant control weaknesses and, if detected, additional work will then be carried out which is directed towards identification of consequent fraud or other irregularities. However, internal audit procedures alone, even when carried out with due professional care, do not guarantee that fraud will be detected and TIAA Ltd examinations as the Authority’s internal auditors should not be relied upon to disclose all fraud, defalcations or other irregularities which may exist.