

Risk, Audit and Governance Committee

25 November 2025

Agenda item number 11

Implementation of internal audit recommendations- Summary of progress

Report by Senior Accountant

Summary

This report gives a summary of progress in implementing Internal Audit recommendations arising out of audits carried out during 2023/24 and 2024/25.

Recommendation

To note the report.

1. Introduction

- 1.1. This report gives an update on implementing the Authority's Internal Audit report recommendations, focusing on outstanding recommendations and timescales to complete outstanding work.
- 1.2. Appendices 1 and 2 give details of the audits carried out in 2023/24 and 2024/25, in particular:
 - Recommendations not yet implemented;
 - Recommendations implemented since the last meeting; and
 - New recommendations since the last meeting.

2. Summary of Progress

- 2.1. The actions on the Port Marine Safety Code – November 2023 have been updated to 31 March 2026 in Table 1. The compliance window is expected to be opened by the Marine and Coastguard Agency (MCA) between January – March 2026. In light of recent changes to the Port, Marine & Facility Safety Code (PMFSC) additional efforts are underway to refine the formatting of the Broads Authority Safety Management System (SMS).
- 2.2. There are no further updates to the actions on the Corporate Governance and Risk Management from February 2024 (table 2) as the Code of Conduct will be updated in December 2025.

- 2.3. The recommendations 1-8 on the Cyber Security Maturity Assessment from March 2025 have been implemented in September 2025. Actions on the recommendation 9 have been updated to 31 December 2025 in Table 3.

3. Internal Audit Programme 2025/26

- 3.1. Since this report to the Committee in July 2025, the first audit agreed by members, for the Tolls System and income collection, started in October 2025 and is expected to last until December 2025. The purpose of of this audit is to seek assurance that the controls in place to manage the toll system and collect toll income are adequate and effective, ensuring that the Authority receives all income due. The results from this audit will be reported to the next meeting in February 2026.
- 3.2. At the last meeting members agreed for the plan for 2025/26 to be amended. Please see agenda item 10 for other proposed audits.

Author: Izabela Foley

Date of report: 06 November 2025

[Broads Plan](#) strategic objectives: All

Appendix 1 – [Summary of actions and responses to Internal Audit 2023/24](#)

Appendix 2 – [Summary of actions and responses to Internal Audit 2024/25](#)

Appendix 1 – Summary of actions and responses to Internal Audit 2023/24

Table 1

Port Marine Safety Code – November 2023

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
<p>4. Review and Audit Action to be taken to ensure that an appropriate compliance statement is made by the Duty Holder when this is next required by the MCA (likely to be in March 2024). This includes ensuring that appropriate reporting mechanisms are in place in line with the recommendations above, to enable the Duty Holder to make such a statement.</p>	Important	Head of Safety Management	<p>We will contact the MCA and discuss the compliance report, the timing and format to ensure we are consistent with other PMSC duty holders.</p> <p>Update: The MCA still needs to open the window to allow compliance to be reported. RR registered with the MCA, and when the reporting window opens, will be notified and able to document the Authority's compliance with the code.</p> <p>The DfT said the new edition PMSC sits with the Minister and awaits Ministerial sign-off and is expected to be published during February or early March. The code will be renamed as the Port and Marine Facilities Safety Code to emphasise the inclusion of non-statutory harbour authority facilities into the code requirements.</p> <p>The MCA detailed the updates to the Guide to Good Practice which they suggested will align better with the structure of the revised Code and said this should be published alongside the Code. However, in terms of</p>	<p>By 31/01/2026 Updated to 31/03/2026</p>

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
			<p>the Duty Holder and Designated Person the key principles of the Code will remain as they currently are now.</p> <p>It is anticipated that the 2025 PMSC Compliance Exercise will be launched six months after the publication of the Code so that ports and their Duty Holder shall have time to consider the new edition Code and associated GtGP and any changes that maybe necessary to make to enhance code compliance</p> <p>Update Jul 2025: The PMSC (a Government guidance standard) has been reviewed by the Government and amended.</p> <p>The new guidance, “Port Marine & Facility, Safety Code”, came into effect in April 2025. The MCA has agreed to open its compliance window in January 2026, meaning the Authority will review the new standard, apply any changes following the Government review, take these changes through the committee structures (BSMG, Navigation Committee & Broads Authority) and report our compliance, as per the audit recommendation at the open window in Jan 2026.</p>	

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
			<p>This open window (Jan 2026) will have been the first opportunity since the PMSC Audit, for the Authority to register our PMSC plan as compliant.</p> <p>Update Nov 2025: The following window to meet compliance of the Broads Authority Safety Management System (SMS) will be opened by the MCA in January-March 2026.</p> <p>External auditors have audited the Authority's SMS, and although it is compliant, its formatting differs from that of other SMSs. This is because the Government changed the PMSC to the Port, Marine & Facility Safety Code (PMFSC) and added a new set of 10 headings. We are using a marine specialist to compile our SMS into a compliant format and hope to meet the new MCA compliance deadline (Jan- Mar 2026)</p>	

Table 2

Corporate Governance and Risk Management – February 2024

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
<p>1. The Local Government Act 1972 Add expectations for attendance and consequences for non-attendance to the Members’ Code of Conduct.</p>	Needs Attention	Head of Governance	<p>This will be reviewed as part of the next members code of conduct update. The next review is due within the next 12 months. Governance will continue to monitor absence and notify members where they maybe in risk of breaching the 6-month rule. It will continue to be highlighted to new members via the terms and conditions.</p> <p>Update: The Code of Conduct is being reviewed by the Standards Committee on 20 February 2025. As part of the review, SGO consulted the Authority’s Monitoring Officer, and his view is that it would not be appropriate to include this in the Code of Conduct. His recommendation is that we include in the Members’ Handbook.</p> <p>SGO confirms that the Broads Authority do monitor attendances, advise members as necessary and the requirement is included in members’ appointment letters.</p> <p>Update Jul 2025: Added to the members handbook. Consequently, to be updated in the Code of Conduct at the end of 2025.</p>	By 31/12/2025

Appendix 2 – Summary of actions and responses to Internal Audit 2024/25

Table 3

Cyber Security Maturity Assessment – March 2025

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
1. Engagement and Training A policy must be in place requiring all staff to receive cyber security and information security training.	Needs Attention	Head of IT	A single IT security policy is now in place	Completed 30/09/2025
2. Asset Management A policy must be in place to require digital assets to be inventoried and accounted for centrally.	Needs Attention	Head of IT	A single IT security policy is now in place	Completed 30/09/2025
3. Architecture and Configuration An IT Security and Network Security policy must be in place.	Needs Attention	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025
4. Vulnerability Management A policy must be in place to cover patching and updates of digital assets.	Needs Attention	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025
5. Identity and Access Management A policy must be in place to cover user authentication and access controls	Needs Attention	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025
6. Data Security A policy/plan must be in place to cover backup and recovery of data.	Needs Attention	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025
7. Logging and Monitoring A policy must be in place to cover the organisation's security logging and monitoring requirements	Needs Attention	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/action	Timetable
<p>8. Supply Chain Security Regular assurance must be obtained from third parties to provide confidence in supplier's security measures and controls.</p>	Important	Senior ICT Support Officer	A single IT security policy is now in place	Completed 30/09/2025
<p>9. Supply Chain Security IT suppliers must be reviewed periodically to ensure that they are meeting contractual security obligations and key performance targets.</p>	Important	Senior ICT Support Officer	<p>Policy will be put in place as recommended</p> <p>Update: This is ongoing. We are working with Cyber GSeC (Government Security Centre for Cyber) and a SoW (statement of works) has been agreed. Cyber GSeC will provide the following deliverables during the lifetime of the engagement:</p> <ul style="list-style-type: none"> • Review the current state: A review of existing due diligence checks and level of maturity. • Advice and guidance: where to find valuable sources of information regarding good practice for supply chain risk • Creation of standard process: advice and guidance with regards developing appropriate checks of suppliers for example, pre-procurement questions, security requirements and schedules, annual compliance checks. • Record keeping advice and guidance with regards to supplier registers and record keeping, to ensure suppliers are tracked and engaged at appropriate times. 	By 30/09/2025 Updated to 31/12/2025