Financial Scrutiny and Audit Committee
24 July 2018
Agenda Item No 12

Implementation of Internal Audit Recommendations: Summary of Progress

Report by Chief Financial Officer

Summary:	This report updates members on progress in implementing Internal Audit recommendations arising out of audits carried out during 2016/17 and 2017/18.
Recommendation:	That the report be noted.

1 Introduction

1.1 It has been agreed that this Committee will receive a regular update of progress made in implementing Internal Audit report recommendations, focusing on outstanding recommendations and including timescales for completion of any outstanding work.

1.2 This report summarizes the current position regarding recommendations arising out of internal audit reports which have been produced for 2016/17 and 2017/18. It sets out in the appendix details of:

- recommendations not yet implemented;
- recommendations not implemented at the time of the last meeting which have since been implemented: and
- New recommendations since the last meeting.

2 Summary of Progress

2.1 In the previous report to this Committee in March the final recommendation relating to External Funding has been completed. Four of the recommendations relating to the Port Marine Safety Code have been completed. Commentary on the outstanding recommendations is provided in Appendix 1.

3 Internal Audit Programme 2017/18 and 2018/19

3.1 The fourth audit from the 2017/18 programme has now been completed, with further details below. The first two audits from the 2018/19 programme are not due to commence until the third quarter of this year. These audits will cover Corporate Governance and Key Controls with Branding and Disaster Recovery due in the final quarter. The outcome of these audits will be reported to the March committee.

3.2 Corporate Governance

3.2.1 The objective of the audit was to review the adequacy, effectiveness and efficiency of the systems and controls being put in place for the General Data Protection Regulation (GDPR) coming into force on 25 May 2018. This resulted in a “reasonable” audit opinion with three “important” and two “needs attention” recommendations.

3.2.2 The audit identified five areas for improvement. Details of these recommendations and their progress can be found in Appendix 1.

3.2.3 Good practice was noted relating to sound controls that are in place and operating consistently:

- A GDPR Compliance Plan has been produced which contains a number of actions to be taken to comply with GDPR requirements. This is monitored and updated by the GDPR Project Group set up in August 2017 to ensure GDPR compliance.
- The Solicitor and Monitoring Officer has been assigned as the Authority's Data Protection Officer and is now a qualified GDPR practitioner having attended and successfully completed the GDPR practitioner course.
- The Authority's privacy statements have been revised to include mandatory information in relation to GDPR requirements.
- Compulsory training sessions for staff have been held in respect of GDPR and further training is scheduled in March and April. Members training is also due to be arranged.

3.2.4 Two of the “important” and the two “needs attention” recommendations have been completed. One “important” remains outstanding but on target for completion by the new revised date.

Background papers:	None
Author:	Emma Krelle
Date of report:	21 June 2018
Broads Plan Objectives:	None
Appendices:	APPENDIX 1 – Summary of Actions / Responses to Internal Audit Recommendations 2016/17 and 2017/18

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2016/17

External Funding: October 2016

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Procedural guidance** To develop procedural guidance for the Broads Landscape Partnership. This procedure should cover the administrative processes, including project management, governance, systems used such as base camp, and the staff involved. The procedures should be version controlled. The compilation of such procedural guidance would enable a consistent approach to be applied with the day to day management of the service. Procedures can also be used as a training tool and to highlight process improvements and efficiencies. This will help to mitigate the risks of inconsistent practices occurring, inefficient and ineffective processes being applied and disrupted business continuity.	Important	Broads Landscape Partnership Programme Manager	Agreed. Procedural guidelines will be produced in draft by the end of January to be presented to the next Board meeting (March) for approval. Update: Following the Board meeting it was agreed to develop procedural guidelines following the submission of the second round application. These guidelines will include management of payments, reporting structure and evaluation requirements. There will also be a contract specific to each project which will include responsibilities related to CDM, insurance, safe-guarding, etc. The board decided that we need to speak to all board members and gather a number of	Originally agreed by 31/01/17 Updated to 31/03/18

Summary of Actions / Responses to Internal Audit Recommendations 2016/17

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
			organisations policies and procedures to allow us to create a bespoke set for the delivery phase of the Scheme. Following the successful submission of the second round application the board has yet to reconvene. A whole new board needs to be appointed who will agree the reporting structures and evaluation requirements. To be completed prior to 31 March 2018 before the first claim is submitted for the delivery phase. The new board is due to meet week commencing 19/02/18. Completed.	

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

Asset Management: August 2017

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Maintenance and insurance** A master record of building condition monitoring surveys is created, to provide assurance that all surveys are completed when required. An overall record of building surveys will provide management with assurance that condition of assets is being monitored and that necessary maintenance tasks are completed. If this kind of overview is not available, it is more difficult to determine whether surveys are being completed. Hence there is a risk that the condition of properties deteriorates, potentially leading to financial and reputational loss to the Authority.	Important	Asset Officer	Conditioning monitoring is dependent on the IT work plan and priorities. A meeting to scope project and timescale to be undertaken by end of September 2017. Update: Although reported complete at the last FSAC the system was taken down so that conditioning monitoring forms were stored against specific building sites. Responsible officers are now beeing informed and DMS will be available for use by the end of July.	Originally agreed by 30/09/17 Updated to 31/07/18
3.	**Leases** The Authority agrees timescales for completing lease agreements with key stakeholders to reduce delays. Agreeing a timescale with all parties involved will help to ensure that key tasks are completed in a timely	Needs Attention	Solicitor & Monitoring Officer	Delayed responses from our current legal provider have been identified. This will be addressed when we go out to tender for Legal Services. The tender is due to go out by the end of September with the new contract to	Originally agreed by 01/04/18 Updated to 28/09/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	manner. If there is no agreed timescale, it is more difficult for the Authority to conclude lease agreements in advance.			start 1 April 2018. New/extension leases are planned 12 months prior to expiry date. Control over the lessee legal services are difficult to influence due to the size and type of their organisations. Update: Due to delays in the procurement process a new provider for legal services has yet to be determined. The preferred option at this stage is to move to a standing list of property legal providers which will need to be agreed by the next Full Authority meeting in September.	

Port Marine Safety Code: September 2017

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Governance** To arrange for a peer review to be	Important	Head of Safety	Agreed. The Authority has considered the issue of	By 31/01/19

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
undertaken of the Broads Authority's Safety Management System (SMS) by the Canal and River Trust, or another suitable organisation, as a reciprocal arrangement in between external audit visits in addition to the 3 yearly external audit. The PMSC Guide to Good Practice advocates that the DP is independent of the SMS process and external / peer reviews would assist in mitigating the risks associated with this. This will also assist in assessing the performance of the SMS through benchmarking against other similar organisations.		Management	independence of the external auditors and the appointed designated person. The Authority is assured that the recent change in external audit providers adequately provides the assurance that the process is independent and complies with the requirements of the Port Marine Safety Code. However the recommendation of using a peer review or a MCA health check will give further assurance of independence. The Authority will commence talks with possible providers, by September 2018, regarding this proposal with the aim of scheduling an interim peer review or Health check in 2019. Update: Initial contact made with both the MCA and an external independent	

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
				consultant who offer PMSC health checks.	
2.	**Governance** To include a PMSC dedicated page on the Authority's website. This should include: - A performance dashboard showing the status of each indicator, detailing the target, current performance against the target and the historic trend. - The Authority's SMS, highlighting the Authority's responsibilities as Duty Holder for the Broads. A dedicated page on the website would increase the awareness and prominence of the PMSC and a consistent approach to reporting performance, mitigating the risk that the PMSC is not complied with and performance of the PMSC is not transparent.	Important	Head of Safety Management, Head of Communications.	Agreed. A dedicated webpage will be developed to pull together the elements that are already published but scattered around the website. This "new" page will allow for the compliance statements to be located where a clear focus exists on the PMSC and the SMS. Completed, please see link below. http://www.broads-authority.gov.uk/boating/navigating-the-broads/safety/port-marine-safety-code	By 31/03/18
3.	**Governance** The Authority's annual report should refer to the PMSC, including compliance with this and the standard of performance, cross referenced to the performance dashboard.	Important	Head of Safety Management, Head of Communications.	Agreed. The Annual report is prepared during the spring of each year and published in the Summer. A statement to reflect the recommendation will be	By 30/09/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	Inclusion in the authority's annual report would increase the awareness and prominence of the PMSC, mitigating the risk that the PMSC is not complied with and performance of the PMSC is not transparent.			included in the next annual report and will feature as a standing item in future reports.	
4.	**Governance** To update the Authority's SMS as follows: - The Introduction chapter to include reference to the commitment of the Broads Authority to comply with the standards laid down within the PMSC; - Reference is made to the harbour revision order being progressed for the transfer of Mutford Lock to the Authority; - Inclusion of an overall section on contractors and their obligations in respect of the PMSC; - Inclusion of the general direction and special direction policies as supported by the Navigation Committee. This will document that the Duty Holder makes a clear published commitment to comply with the standards laid down in the Code. Clearly documented obligations of	Important	Head of Safety Management	Agreed. The SMS will be updated during the winter of 2017 for adoption by the Authority at its meeting in March 2018. All of the recommended changes and additions will be included in the new version 7 of the SMS. Completed.	By 31/03/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	contractors mitigates the risk that contactors do not comply with the code. Inclusion of relevant policies and harbour orders mitigates the risk that the authority's powers and procedures are not transparent.				
5.	**Governance** To formalise the reporting of internal audits by the Head of Safety Management to the appropriate committees / groups, e.g. the BSMG including the annual schedule / Internal Audit Programme of audits. To ensure these cover all aspects of the PMSC. The BSMG would receive assurance that the SMS is reviewed against all aspects of the PMSC mitigating the risk that some areas may not be in compliance.	Needs Attention	Head of Safety Management	Agreed. SMS audits for 2017 will be reported to the Boat Safety Management Group in Jan 2018, Navigation Committee Feb 2018 and to the duty holders in March 2018. The SMS will be updated to reflect this formal reporting requirement at its next issue in March 2018. Completed.	Originally agreed by 31/03/18 Updated to 31/05/18
7.	**Governance** Briefings given to the Navigation Committee and BSMG on the risk assessment process, hazard identification and assessment and the ALARP principle are documented and recorded in the minutes. Briefing packs in relation to the risk	Needs Attention	Solicitor and Monitoring Officer, Head of Safety Management	Agreed. All members of Boat safety management group, the stakeholder hazard review group, the navigation committee and the Broads Authority receive training on risk assessment and ALARP principles	By 28/02/19

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	assessment process, hazard identification and assessment and the ALARP principle (which are provided to the stakeholder group involved in the review of hazards) should also be made available to all new appointees to the Navigation Committee and the BSMG. Consideration is also given to providing these to all members of the Navigation Committee and the BSMG. A record of all training provides confirmation that it has taken place and reduces the risk that misinformed decisions are made resulting in inadequate port marine safety.			before dealing with the risk assessments process. This formal training will be recorded in the minutes of each of the groups/ committees at the next opportunity when hazards are reviewed/ assessed scheduled for Feb 2019 Any new members to the group will be trained in this regard prior to any risk review or assessment as part of the regular refresher training being delivered each time the risk review process is entered into.	
9.	**Hazards** To review the SMS risk categories / criteria of people, environment and assets against the four criteria of: life, environment, business (reputation) and damage (port and shipping), as contained in the latest PMSC Guide to Good Practice. The risk categories/criteria will be based on the latest PMSC Guide to Good Practice mitigating the risk that	Needs Attention	Head of Safety Management	Agreed. A review of assessment criteria will be carried out by the Boat Safety management Group at its meeting in March 2018. Any “new” criteria will be used as the basis for the next formal stakeholder hazard review in February 2019.	By 31/03/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	the consequences of risks/hazards are not appropriately assessed and mitigated as required.			Update: Proposed assessment criteria are set out in the draft update to the Safety Management System, BSMG are being consulted as part of the SMS update. It is proposed that the new criteria will be considered by the Authority in March 2018 Completed.	

Key Controls: December 2017

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
3.	**Budgetary Control** The limit for reporting on variances identified through budget monitoring is reviewed and reduced if necessary, to reduce the risk of potentially significant variances going unchallenged. The review could consider introducing a percentage in addition to an amount. Reviewing the limit for variances will	Needs Attention	Chief Financial Officer	Agreed for a review to be undertaken with members whilst taking into account variance reporting levels at other National Parks. Completed. Review of other National Parks undertaken and agreed to keep reporting at current limit of +/- £10k. Budget holders will	By 31/03/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	ensure that it is set at an appropriate level so that all significant variances are addressed. If this threshold is not reviewed, then there is a risk that some significant variances will not be challenged or reported on.			provide monthly commentary on +/- £5k which will be reviewed with Directors from the new financial year.	
4.	**Accounts receivable** The Scheme of Powers Delegated to Officers is updated to remove outdated references to the Treasurer and Financial Advisor to the Authority and to replace them with current references including the Chief Financial Officer (Section 17 Officer). Updating the Scheme of Powers Delegated to Officers will align governance arrangements to the Authority's current officer structure. If the document is not up to date, there is a risk of confusion over the decision making arrangements which could also lead to decisions being made by unauthorised members of staff.	Needs Attention	Solicitor and Monitoring Officer	Agreed. Scheme of Powers to be updated and adopted by the Authority. Update: Amended scheme of powers will be considered by the Broads Authority on 27/07/18	Originally agreed by 16/05/18 Updated to 27/07/18

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

Corporate Governance: March 2018

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
1.	**Compliance** The authority's existing Information Retention Policy and the ICT Communications Policy (and any other policies , if relevant) to be reviewed and updated to include the approach to the technical and security measures in place and the ongoing review of them to ensure compliance with the GDPR. Policies to include data cleansing (data retention, minimisation and accuracy) and how this is carried out on an ongoing basis for all types of files including online systems, data on drives, paper files, data in other formats, and emails (shared/own drives). Policies should refer to the data asset register which verifies data cleansing undertaken and include a timetable for conducting data cleansing on a timely basis. Explicit reference to be made to the GDPR and the Data Retention and Information Management Policy to be uploaded onto the authority's website.	Important	Solicitor and Monitoring Officer	Agreed. Completed.	By 30/04/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	The review and update of existing policies is a way of ensuring all key areas/requirements of the GDPR are covered and provide consistent processes for data collection, validation and cleansing. This mitigates the risk of non-compliance with the GDPR specifically article 32 - security of processing and the new accountability principle in Article 5(2) to demonstrate compliance with the principles of the GDPR.				
2.	**Compliance** The data asset register incomplete columns to be finalised and to take into account the ICO checklists for 'Documentation of processing activities – requirements' and 'Documentation of processing activities – best practice; and ICO documentation template for controllers. This should include, but not be limited to the following: - The source of the personal data; - Legal basis for processing data; - Plan for return and destruction of the data once processing is complete	Important	Solicitor and Monitoring Officer	Agreed. With the exception of the plan for the return and destruction of data column this is complete. Terms have recently been agreed with the Payroll processors in this regard and the final version of the data asset register will be submitted to Internal audit during the week commencing 9 July 2018.	Originally agreed by 30/04/18. In hand for completion by 31st July 2018.

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	(shared data); - Occupational health records; - The name and contact details of your organisation (and where applicable, of other controllers, your representative and your data protection officer); and - Description of technical and organisational security measures (including records, devices, emails, which are encrypted) Adhering to ICO checklists and the documentation template should assist in ensuring mandatory information is included, best practice is followed and terminology and approach is consistent with the ICO. This thereby mitigating the risk that there is non-compliance with the GDPR.				
3.	**Compliance** The GDPR compliance plan to be updated to include: - Production of a 'light touch' DPIA template for more simple processes/data which do not require a full DPIA assessment. - Timeline for applying full DPIAs to the areas identified as requiring them	Important	Solicitor and Monitoring Officer	Agreed. Completed.	By 30/04/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	- DPIA requirements are built into existing processes (for project management and risk management) for new projects and new systems, etc. in accordance with the GDPR requirements. The above actions should take into account the ICO Conducting Privacy Impact Assessments Code of Practice including the screening questions which help organisations identify whether a DPIA is needed; and the DPIA template includes actions which can be taken to reduce the risks, and any future steps which would be necessary. These actions should be accompanied by implementation dates. The ICO has promoted the use of DPIAs as an integral part of taking a privacy by design approach and inclusion of these within the GDPR compliance plan should reduce the risk that processes/data are not assessed sufficient leading to non-compliance with the GDPR.				
4.	**Compliance** The general privacy statement title	Needs Attention	Solicitor and Monitoring	Agreed.	By 30/04/18

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

	Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
	heading - 'Your rights in relation to data processing including rights to access' to specifically state the right to erasure. The narrative within this section refer to the specific element of the GDPR (i.e. article 17) and the extra requirements when the request for erasure relates to children's personal data. Specific reference to the right to erasure in the general privacy statement makes this clear and mitigates the risk that this right is overlooked by the general public/users of the website and the authority is not clearly demonstrating compliance in a transparent manner.		Officer	Completed.	
5.	**Compliance** The Data Protection Officer (DPO) to notify the Finance Scrutiny and Audit Committee (FSAC) that a review of the GDPR corporate risk will be undertaken at the end of March 2018 to ascertain if the risk is being mitigated as planned and that the authority will be compliant by the time it comes into force in May.	Needs Attention	Solicitor and Monitoring Officer	Agreed. Completed. Risk Register to be considered by FSAC at the November meeting.	N/A

APPENDIX 1

Summary of Actions / Responses to Internal Audit Recommendations 2017/18

Recommendations	Priority Rating	Responsible Officer(s)	BA Response/Action	Timetable
Reviewing the corporate risk in a timely manner helps mitigate the risk that the authority will not be compliant with the GDPR when it comes into force on the 25 May 2018.				