**Audit and Risk Committee**
5 March 2019
Agenda Item No 11

# 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 2017/18 and 2018/19. |
| **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 summarises the current position regarding recommendations arising out of internal audit reports which have been produced for 2017/18 and 2018/19. 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 December the outstanding recommendations relating to the 2017/18 audits (Asset Management and the Port Marine Safety Code) remain unresolved. Updated commentary on the outstanding recommendations is provided in Appendix 1.

## 3 Internal Audit Programme 2018/19

3.1 The first three audits from the 2018/19 programme have now been completed, with further details below. The fourth audit on Branding is due to start 28 February with its results reported to the next committee in July 2019.

### 3.2 Key Controls

3.2.1 The objective of this audit was to look at the fundamental systems that feed into the statement of accounts to provide assurance on the key controls. The areas reviewed as part of the audit were; Treasury Management/Investments, General Ledger, Asset Management, Budgetary Control, Accounts

Receivable, Accounts Payable, Payroll, Toll Income, Control Accounts, and follow up of Internal Audit Recommendations. This resulted in a “substantial” audit opinion with no formal recommendations being raised.

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

- Investments tested were documented and authorised.
- Loans and investments are reconciled to the general ledger and bank statements.
- Journals are raised sequentially and approved independently.
- The general ledger suspense account is reviewed on a monthly basis and any long outstanding items are cleared.
- All capital additions and disposals reviewed were authorised in accordance with procedures.
- A quarterly report of expenditure is downloaded from the ledger and reviewed for items to be capitalised.
- The asset register is reconciled to the ledger once a year and access to the register is restricted to appropriate staff.
- Budget monitoring reports are shared with budget holders on a monthly basis, from the end of the first quarter, which highlights any variances above £5,000. These are accompanied by an email from the Financial Accountant requesting an explanation of variances and changes to forecast outturn (year-end positions); commentary to explain significant variances (+/- £5,000) within their budgets and; requests for budget virements (budget transfers).
- Budgetary information, both capital and revenue is reconciled to the general ledger on a monthly basis.
- Invoices are independently checked prior to posting to the ledger.
- All invoice payments require two stage authorisation, thereby ensuring that only accurate and approved payments are processed.
- BACs runs had been signed and dated, prior to the payment run, by an appropriate officer.
- Starters, leavers and amendments to the payroll are checked to ensure that they have been actioned correctly by the payroll provider, thus ensuring the Authority’s payroll is accurately maintained.
- There is a clear audit trail of actions taken to recover unpaid tolls, ensuring that debt recovery follows a prescribed and effective process and with all monies due to the Authority being pursued / received.
- Toll payments can be checked on the Tolls Management System by Rangers in the field, reducing the Authority's costs for printing plaques.

### 3.3 Corporate Governance and Risk Management

3.3.1 The objective of the audit was to review the adequacy, effectiveness and efficiency of the systems and controls in place over Corporate Governance and Risk Management. This resulted in a “reasonable” audit opinion with two “important” and five “needs attention” recommendations. These recommendations can be found in Appendix 1.

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

Risk Management

- The Strategic Risk Register (SRR) is kept up to date through six monthly reviews by the Monitoring Officer and Management Forum. It is then reported to the Audit and Risk Committee (ARC) thereby assisting the Broads Authority to meet the requirements of its Code of Corporate Governance, specifically in managing risks and performance.
- Partnership related risks are assessed on an ongoing basis and are included on the SRR. An annual report on partnership arrangements is reported to the Full Broads Authority. This report provides details of the Strategic Partnerships which are currently registered with the Broads Authority and highlights which actions are required to address weaknesses and in so doing, the Broads Authority manages risks in this area.

GDPR

- Recommendations from the previous GDPR audit (BA1804) have been verified as complete and are confirmed as still in operation. A GDPR risk is included on the SRR and controls recorded as in place to mitigate this risk comprise of a GDPR action/compliance plan and a GDPR working group.

3.3.3 One “needs attention” recommendation has been completed. The remaining six recommendations remain outstanding but on target.

### 3.4 Disaster Recovery

3.4.1 Disaster Recovery (DR) was an area that had not previously been audited at Broads Authority. As the systems that support the Authority's DR processes have been moved to the Dockyard at Griffin Lane, Norwich. The facility itself has been renovated and extended to support this work. As a result of this the DR plan has been updated. This objective of the audit was to help provide assurance that the appropriate controls are in place. This resulted in a “reasonable” audit opinion with one “important” and four “needs attention” recommendations. These recommendations can be found in Appendix 1.

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

- There is a documented Disaster Recovery (DR) plan document that has recently been reviewed to take account of recent improvements made to the DR facilities. It is also shared amongst relevant IT staff. Periodic review and communication of relevant plans reduces the risk that the plans are not fit for purpose and not shared as appropriate.
- Responsibility for DR is shared between the Head of IT & collector of Tolls and the Senior ICT Support Officer with assistance as required from other IT staff. The shared responsibility reduces the risk of relevant plans and operational procedures not being fit for purpose.
- The DR plan includes appropriate invocation and escalation procedures in support of similar processes and procedures within the Business Continuity

Plan. These reduce the risk of a lack of a coordinated response to DR incidents.

- The audit noted a lack of historic DR testing, although this is being addressed through the documentation of a proposed DR test plan within the DR plan document that has undergone recent review. The process has already started with a small test recovery of a server at the Dockyard as part of the recent DR facility improvement work. The creation of DR test plans will help to demonstrate the viability of the DR infrastructure and related processes.
- The audit noted the ability to divert telephone calls from Yare House to the Dockyard office, which helps to ensure continuity of customer service during an incident.
- The audit noted the presence of external CCTV coverage, which is recorded and retained for 10 weeks. CCTV coverage helps to detect unauthorised access to the Dockyard site.
- The entrance to the Dockyard DR facility did not have a lock fitted, although it was also noted that there is ongoing work to resolve this to help ensure the physical security of the facility.
- The lack of Uninterruptible Power Supply (UPS) at the DR facility is being addressed. This will help to ensure the controlled shutdown of the DR infrastructure following a power outage. UPS facilities provide a temporary battery backup that provides a 'window of opportunity' to power down all relevant equipment in a controlled manner prior to power being restored.

3.4.3 All of the recommendations remain outstanding but on target.

| | |
|---|---|
| Background papers: | None |
| Author: | Emma Krelle |
| Date of report: | 18 February 2019 |
| Broads Plan Objectives: | None |
| Appendices: | APPENDIX 1 – Summary of Actions / Responses to Internal Audit Recommendations 2017/18 and 2018/19 |

**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 |
|---|---|---|---|---|---|
| 3. | **Leases**<br>The Authority agrees timescales for completing lease agreements with key stakeholders to reduce delays.<br><br>Agreeing a timescale with all parties involved will help to ensure that key tasks are completed in a timely manner.<br><br>If there is no agreed timescale, it is more difficult for the Authority to conclude lease agreements in advance. | 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 start 1 April 2018.<br><br>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.<br><br>Update: Following the previous delays with the procurement process and the Solicitor & Monitoring Officer moving to one day a week, legal services within the Authority needs to be re-scoped and this will include property issues. It is still the | Originally agreed by 01/04/18<br><br>Updated to 17/05/19 |

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

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | | | | preferred option at this stage is to move to a standing list of property legal providers. This did not make the previous Authority meeting in February. It will still need to be agreed by the next Full Authority meeting in May. | |

**Port Marine Safety Code: September 2017**

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| 1. | **Governance**<br>To arrange for a peer review to be 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.<br><br>The PMSC Guide to Good Practice advocates that the DP is independent of the SMS process and external / peer reviews would assist in | Important | Head of Safety Management | Agreed. The Authority has considered the issue of 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. | By 31/01/19<br><br>Updated to 30/06/19 |

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

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | mitigating the risks associated with this. This will also assist in assessing the performance of the SMS through benchmarking against other similar organisations. | | | 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.<br><br>Update: Initial contact made with both the MCA and an external independent consultant who offer PMSC health checks. Health check scheduled for mid 2019. | |
| 7. | **Governance**<br>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.<br>Briefing packs in relation to the risk assessment process, hazard | 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 before dealing with the risk | By 28/02/19 |

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

| Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|
| 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.<br><br>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. | | | 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<br>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.<br><br>Update: Briefing pack now in preparation for the forthcoming hazard review in February 2019 | |

**APPENDIX 1**

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

### Corporate Governance and Risk Management: February 2019

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| 1. | **Risk Management**<br>The Risk Management Policy is reviewed and updated as required to reflect the current governance arrangements and responsibilities for risk, including those assigned to the Audit and Risk Committee (ARC) and the frequency of the reporting of risks to the ARC. This should include an explanation of what is classed as an operational risk as opposed to a strategic risk and how service risks should be managed and escalated to strategic level, if required. It should also define the risk appetite/tolerance level.<br>The policy should be version controlled, approved by the Full Broads Authority and reported to the ARC.<br>Following approval, the policy should be disseminated to all staff and placed on the authority's intranet.<br><br>An up to date risk management policy mitigates the risk that out of date | Important | Solicitor & Monitoring Officer | The risk management policy will be reviewed and updated to reflect the correct committee, lead officer and risk appetite (including colour coding). The updated policy will be taken to Audit and Risk for review prior to Broads Authority approval | By 26/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | processes are being used leading to incorrect decision making and lack of corporate governance. | | | | |
| 2. | **Risk Management**<br>An exercise is undertaken to review the Strategic Risk Register (SRR) to identify which risks are strategic, i.e., risks to the achievement of the strategic objectives. This should conclude that the remaining risks are at an operational/service level and as such, should be managed at this level.<br>The resulting SRR should score all risks which have been identified and include a column which states which strategic objective they relate to. In addition, the SRR should make it clear which risks are within and outside of the risk appetite by using colour coding.<br><br>Clearly distinguishing between operational/service level risks and strategic risks helps to ensure that risks are identified on both a service and strategic level allowing for proper understanding of the authorities risk profile and allows for the appropriate | Important | Solicitor & Monitoring Officer | Review to be undertaken with Management Forum to distinguish between operational & strategic risk and how they link with the Strategic priorities in conjunction with the risk policy above. | By 10/06/19 |

**APPENDIX 1**

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | prioritisation of mitigation actions. | | | | |
| 3. | **Risk Management**<br>A review and update of the RM page on the authority's intranet is undertaken incorporating any revised documents such as the RM policy and including relevant committee reports. This should be re-launched with staff including ascertaining feedback on the RM process and identifying any training needs at all levels across the authority. The intranet should provide clarification of what the risk appetite is and how risks, which are outside of the risk appetite, are managed.<br><br>Staff being adequately informed and trained in respect of risk ensures that that correct processes are followed leading to informed decisions being made that assist in the achievement of objectives. | Needs Attention | Solicitor & Monitoring Officer | Following committee approval of the revised policy and register the intranet page will be refreshed and communicated to all staff. | By 16/08/19 |
| 4. | **Risk Management**<br>A standard risk implications section to be introduced on the committee report template to allow for a fuller explanation of the risks. Guidance/criteria to be produced to enable authors to sufficiently assess if | Needs Attention | Solicitor & Monitoring Officer | Agreed and partially completed.<br>Template has been updated and is available on the intranet and the guidance will be completed by July 2019. | By 31/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | there are any risk implications. Guidance to include reference to the SRR and any operational/service risks which have been identified; and the risk management policy.<br><br>A fuller explanation of risks within reports will encourage a risk aware culture within the authority, and a consistent approach is applied in identifying risk implications. Referral to corporate risk documents should alert authors to risks which they may not have been aware of and reduce the risk that objectives are not achieved. | | | | |
| 5. | **Risk Management**<br>The 'Review of the Strategic Risk Register (SRR) reports to the Audit and Risk Committee to contain an explanation of risks that have changed from the previous SRR, including risks which have had their score reduced; risks which have been reduced to the risk appetite; and change of risk description (i.e. the GDPR risk).<br>This should include explanation as to why certain risk scores have not | Needs Attention | Solicitor & Monitoring Officer | Agreed. Audit & Risk report to provide explanation of movements at next review. | By 23/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | lowered from initial risk to revised risk score despite current mitigating actions and additional actions being put in place.<br><br>Providing an explanation for key changes within the committee reports mitigates the risk that the committee does not receive a full picture of the status of risks and if they are being mitigated as expected. | | | | |
| 6. | **Risk Management**<br>A scoring criteria is defined for low, high and medium risks, in relation to severity/impact, for categories such as financial, reputation and service provision.<br><br>A scoring criteria is also defined for low, high and medium risks in relation to likelihood, i.e. a high likelihood applies to a risk likely to happen more than once per year and a low risk is only likely to happen in 10–15 years' time.<br><br>Defining the scoring categories helps assess risks more accurately and reduces the risk that that risks are not | Needs Attention | Solicitor & Monitoring Officer | Agreed. Scoring criteria will be incorporated into the risk policy. | By 10/06/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | appropriately assessed and assigned proportionate mitigation actions. | | | | |
| 7. | **GDPR**<br>Evidence that the payroll provider has implemented the Information Commissioner Office (ICO) recommendations, since the data breach incident, is requested.<br>In addition, all data breaches, including those which have been formally reported and those which the ICO have been consulted on, to be centrally recorded.<br><br>Implementation of ICO recommendations by external organisations, provides assurance that the associated risk are mitigated to an acceptable level and the same breach does not happen again.<br>A central record of all data breaches, which is accessible to key members of staff, mitigates the risk that records cannot be accessed in the event of staff absence and that there is an incomplete audit trail of breaches and subsequent action taken. | Needs Attention | Solicitor and Monitoring Officer | Agreed and completed. Response received from payroll provider on 24/01/19 and redacted e-mail from them supplied. | Completed |

**APPENDIX 1**

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

### Disaster Recovery: February 2019

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| 1. | **Alignment with Business Continuity Plans**<br>The Authority to ensure that senior management are made aware that Business Continuity recovery timelines of up to 24 hours may not be achievable if such recovery has to be undertaken using the tape backups stored at the Dockyard. Formal acceptance (or otherwise) of this risk to be formally documented to support this.<br><br>Formally notifying senior management of the potential inability to support Business Continuity recovery timelines up to 24 hours where a tape restoration is required will help to ensure that the acceptance (or otherwise) of this risk is formally documented.<br>Where senior management are not advised of the potential inability to support Business Continuity recovery timelines up to 24 hours, there is an increased risk that the Business Continuity plan cannot adequately | Important | Head of IT & Collector of Tolls | Agreed | By 31/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | support priority services. | | | | |
| 2. | **Backup and Recovery Capabilities**<br>The Authority to look at options for enhancing the existing data replication service such that it covers priority services such as Finance and Tolls.<br><br>Increased replication between Yare House and the Dockyard will help to ensure timely recoveries of priority services following an incident, including any incidents that render Yare House inaccessible and which would currently require a recovery from tape.<br>Where a tape recovery is required, there is an increased risk that this would result in up to 48 hours of data needing to be re-input as part of the recovery process, given that it takes an average of 24 hours to complete a tape backup at present | Needs Attention | Head of IT & Collector of Tolls | Agreed | By 31/07/19 |
| 3. | **DR Testing**<br>The authority to ensure that all DR tests are formally documented in test reports that are communicated to relevant senior management and which are used as a basis for | Needs Attention | Head of IT & Collector of Tolls | Agreed | By 31/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | updating DR plans with lessons learned using appropriate change control processes.<br><br>The formal documentation of all DR tests into test reports will help to demonstrate that the DR facilities and processes adequately support the Authority's priority services following an incident and that any lessons learned are taken account of as updates to the processes concerned. Where DR tests are not formally documented into test reports, there is an increased risk that the DR facilities and processes cannot be shown to be adequate and that any weaknesses in the DR facilities and processes are not detected and resolved in a timely manner. | | | | |
| 4. | **DR Development for New Systems**<br>The Authority to ensure that relevant Project Management processes are updated to include work to understand what the DR support requirements will be for any new or changed infrastructure.<br><br>The inclusion of work to understand | Needs Attention | Head of IT & Collector of Tolls | Agreed | By 31/07/19 |

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| | Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|---|
| | the potential DR support requirements of any new or changed systems will help to ensure that any changes to the Authority's systems are adequately support as required by the Business.<br>Where DR requirements are not taken account of adequately in project workflows, there is an increased risk that the DR support requirements that may result from the changed infrastructure are not supported adequately following an incident. | | | | |
| 5. | **Dockyard Physical Access Controls**<br>The Authority to ensure that the server rack that contains the DR infrastructure at the Dockyard is moved to a more appropriate location within the DR facility as soon as practically possible.<br><br>Moving the server rack to a more appropriate location will help to ensure the security of the rack and the environmental conditions within the room.<br>If the server rack is not moved to a more appropriate position within the | Needs Attention | Head of IT & Collector of Tolls | Agreed | By 31/07/19 |

**APPENDIX 1**

## Summary of Actions / Responses to Internal Audit Recommendations 2018/19

| Recommendations | Priority Rating | Responsible Officer(s) | BA Response/Action | Timetable |
|---|---|---|---|---|
| DR facility, there is an increased risk of security vulnerabilities caused by the removal of the side panels which has been done to facilitate the operation of the Air Conditioning unit. | | | | |