Audit and Risk Committee

26 July 2022
Agenda item number 13

Implementation of internal audit recommendations summary of progress

Report by Director of Finance

Summary

This report gives a summary of progress in implementing Internal Audit recommendations arising out of audits carried out during 2018/19, 2019/20, 2020/21 and 2021/22.

Recommendation

To note the report.

Contents

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, 2 and 3 give details of the audits carried out in 2018/19, 2019/20 and 2020/21, 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. Since the previous report to this committee in February, the final two recommendations of the Branding audit from 2018/19 have been completed. Three of the recommendations relating to the Port Marine Safety Code and two from the HR and Payroll audit have also been completed. The impact of COVID-19 and workloads have meant that some actions have been further delayed. These have been updated in the appendix. The rest remain as scheduled.

3. Internal Audit Programme 2021/22 and 2022/23

3.1. Since this report to committee in February the final three audits on Key Controls, Corporate Governance and Risk Management and Cyber Security audits have now been completed. The first audit from the 2022/23 plan, Corporate Health and Safety, has been carried out and the draft report is awaited. The result of this will be reported to this Committee in November 2022.

4. Key Controls

4.1. The objective of this audit was to review the fundamental systems that feed into the Statement of Accounts to provide assurance on the key financial controls. The areas reviewed as part of the 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. This resulted in a "substantial" audit opinion with one "needs attention" recommendation being raised (see Appendix 4).

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

- 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.

4.3. The recommendation, as detailed in appendix 4, is currently being investigated.

5.   Corporate Governance and Risk Management

5.1. The objective of this audit was the annual review of governance and risk management which is carried out to support the Head of Internal Audit Opinion. The 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 the review they considered governance arrangements for decision making and the accountability and monitoring of performance during the Covid-19 Pandemic. The review also provides assurance over the Risk Management framework to give a view as to whether it has supported the achievement of strategic priorities. This resulted in a "reasonable" audit opinion, with one "important" and five "needs attention" recommendations being raised (see Appendix 4).

5.2. Good practice was noted relating to sound controls that are in place and operating consistently. Those relating to Governance arrangements for decision making were:

- 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.

5.3. Those relating to Performance Monitoring were:

- 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.

5.4. Those relating to the Risk Management Framework were:

- 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.

5.5. Whilst Management Team disagreed with two the recommendations, the remaining four have been completed.

6. Cyber Security

6.1. The objective of this audit was to carry out the maturity assessment 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. This resulted in a "reasonable" audit opinion with two "important" and four "needs attention" recommendations (see Appendix 4). Although the report was in draft at the time of writing Management have confirmed the responses set out in appendix 4.

6.2. The format of this audit is slightly different to that of the two audits in paragraph 4 and 5. The ICT team completed a self-assessment against each of the ten areas above and this was reviewed by TIAA's Cyber Assurance team. It was noted that the audited maturity levels shown reflects 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.

6.3. It was also noted that the Authority has not experienced any cyber incidents within the last 12 months.

6.4. TIAA's Cyber Maturity model is based on the traditional maturity model, and comprises of levels 0-5 as described in the table 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 organisations.
4	Quantitative	Measured and controlled process.
5	Optimising	Focus is on continuous process and improvement.

6.5. TIAA's maturity assessment is summarised in the radar diagram below. Significant gaps of 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.

Broads Authority Cyber Security Maturity Assessment
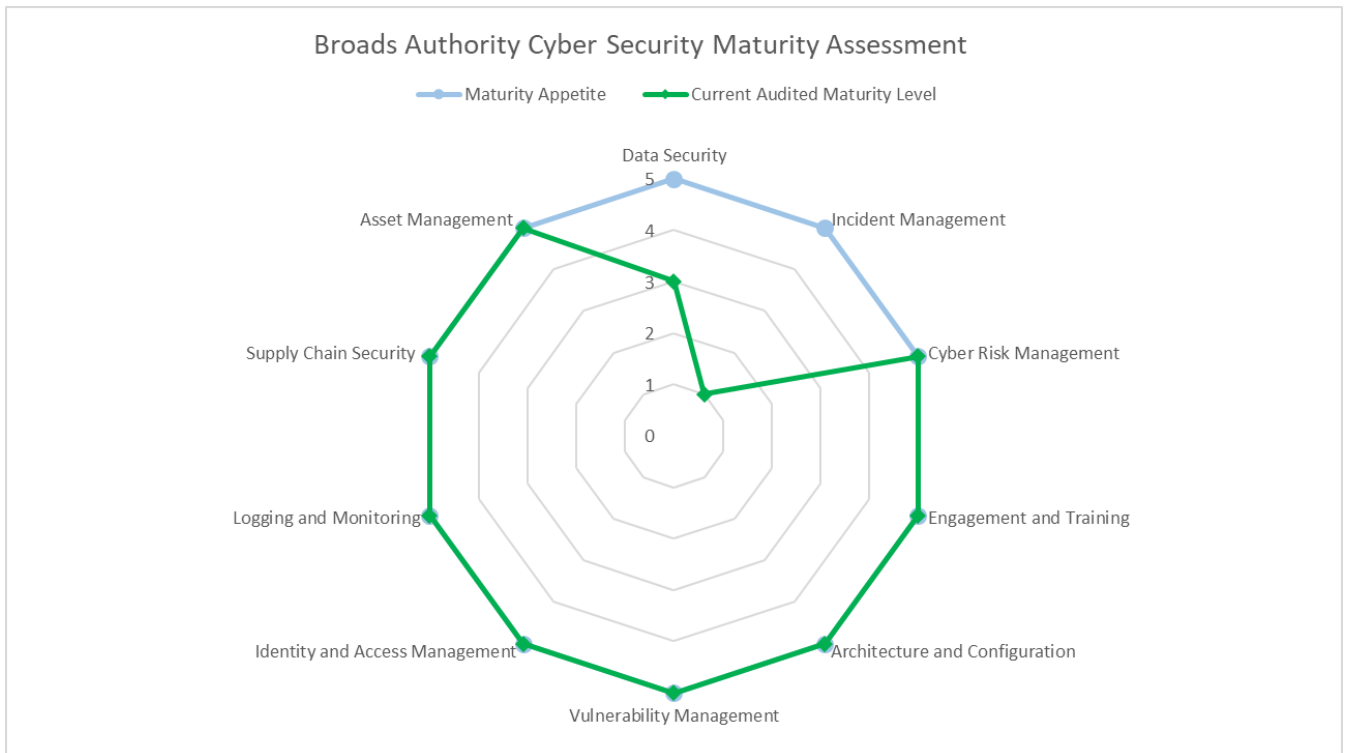
6.6. The recommendations remain on target for completion.

Author: Emma Krelle

Date of report: 08 July 2022

Appendix 1 – Summary of actions and responses to Internal Audit 2018/19

Appendix 2 – Summary of actions and responses to Internal Audit 2019/20

Appendix 3 – Summary of actions and responses to Internal Audit 2020/21

Appendix 4 – Summary of actions and responses to Internal Audit 2021/22

Appendix 1 – Summary of actions and responses to Internal Audit 2018/19

Table 1

Branding - April 2019

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
2. Broads Authority branding - strategies, guidelines / procedures The Broads Authority Communications Policy be updated to include the roles and responsibilities for overseeing management of correct branding. This should be included within a separate branding section which the policy does not currently have. This should make the branding area more easily to locate within the policy and helps mitigate the risk that responsibilities for branding are unclear.	Needs Attention	Head of Communications	New communications strategy delayed by COVID comms activity but many elements completed and anticipate strategy will be in place by end Sept 2022 Update: New 'branding' area on intranet developed that incorporates updated and new documents, including: • Communications Team Guide • BA Brand guidelines • BA brand guidelines supplement • BA language style guide • Words commonly used in BA publications • BA signs guide	By 31/10/19 Updated to 30/09/22

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
			• Logos and templates for letterheads, reports and PowerPoint presentations. • Instructions for email signatures All elements of the strategy are complete and available on the intranet. We intend to complement this with and over-arching strategy document by October 2022. Completed.	
5. Broads Authority branding - use of the Broads Authority logo A review and update of the communications page on the Authority's intranet be undertaken once the national parks' branding strategy and associated documents, including the local broads national park strategy and Broads Authority Communications Policy, are finalised. This should be re-launched with staff including the provision of staff and member training in relation to branding, incorporating the use of both the Broads Authority logo and Broads National Parks logo.	Needs Attention	Head of Communications	Agreed. Intranet content to be produced in conjunction with strategy, guidelines and procedures. Awaiting completion of new communication strategy (see recommendation two above) The intranet now features a 'branding section' which includes a 'guide to the comms team' This document is used as a comms induction for all new starters to	By 31/10/19 Updated to 30/09/22

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
The communications intranet page should include the communications team details; branding strategies and communications policy; and the Broads Authority New Signs guide.			the organisation. The Branding section also includes logo's, brand guidelines, brand narratives, sign guide, language guide as well as presentation and document templates to ensure correct branding and accessibility rules can be applied. Completed.	

Appendix 2 – Summary of actions and responses to Internal Audit 2019/20

Table 2

Procurement – December 2019

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
7. Procurement Procurement training is provided to all relevant members of staff, and Members, where applicable. Up to date procurement training ensures that staff are aware of and are adhering to the correct guidelines, thereby mitigating the risk of non-compliance with CSOs and OJEU requirements	Needs Attention	Chief Financial Officer	Agreed. Update: Delayed originally due to ongoing work on COVID-19 response, the Statement of Accounts and budget preparation for 2021/22. This has been further delayed by this year's	By 30/06/20 Updated to 30/09/22

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
			audit, 2022/23 budget planning and a number of vacancies within the Finance Team. Vacancies within the team have continued since March 2021 but the last post should be filled by the end of January. Once all new members of the team are fully trained then the training will be prioritised and delivered.	

Appendix 3 – Summary of actions and responses to Internal Audit 2020/21

Table 3
Governance and Risk Management – March 2021

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
2. Changes to committee meetings 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. This mitigates the risk of not having a completed audit trail in place resulting in key items of business/decisions being missed if deferred matters are not assigned to the next convenient meeting.	Needs Attention	Head of Governance	Agreed. Notes added to deferred items. Update: 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.	By 31/12/2021 Updated to 31/12/2022

Table 4

Port Marine Safety Code – June 2021

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
1. Governance 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. This helps reduce the risk that performance of the PMSC is not reported in a consistent and timely manner leading to ambiguity over whether the PMSC is performing well and meeting targets as planned.	Important	Head of Safety Management	Agreed. Update: Please note that this recommendation was previously marked as complete in July 2021, but a further review of documents highlighted it was out of date. 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 wok in progress, a meeting has been 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.	By 31/10/2021 Updated to 31/01/2023
2. Governance	Important	Head of Safety Management	Statement being updated to reflect recent changes following	By 31/10/2021

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
The three-yearly statement of compliance with the code be signed and retained on file for future reference. This assists in mitigating the risk that the authority dose not formally review compliance on a three-year basis as prescribed.			audit. BA Chair to agree and sign completed statement. Update: Following (draft) recommendations within the MAIB report into aspects of the Safety Management System a fuller review of key aspects within the PMSC are now required. A new compliance date is given to reflect this additional work. Completed.	Updated to 30/06/2022
3. Pilotage The General Direction for larger vehicles and navigation on works Guidance be finalised. This helps mitigate the risk that sufficient navigation rules are not in place and navigation of the broads is not managed as effectively and safely as required, in relation to larger vehicles.	Important	Head of Ranger Services	General Directions are rarely used by Broads Authority - most directions are 'Special'. This requirement will require legal inputs and cost benefit analysis to assess its viability. Current requirements are met using Special Directions. Update: Due to limited use of General Direction (due to lack of commercial traffic) and more	By 31/10/2021 Updated to 28/02/2023

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
			pressing Ranger Team safety priorities, this recommendation had been deferred into 2022/23 financial year.	
4. Governance PMSC related documents and files, location and storage (both electronic and hardcopy) is reviewed to ensure these can be accessible to relevant members of staff on a timely basis. This helps mitigate the risk that key documents cannot be located in a timely manner leading to gaps in the safety management system.	Needs Attention	Head of Safety Management	Files and documents being migrated to DMS. New MARNIS (Port marine management software) being implemented will assist with data collection and reporting. Update: Trials of the MARNIS system (electronic PMSC filing and recording system) has identified software issues that have been slow to resolve due to Covid and the need to re-engage the manufacturer. More testing is taking place in the hope to resolve these glitches. Completed.	By 31/10/2021 Updated to 30/06/2022
6. Governance The documents, reference numbered within the Broads Authority (BA) PMSC, are reviewed to ascertain their	Needs Attention	Head of Safety Management	Review to be undertaken.	By 31/10/2021

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
location and to appraise whether they are still relevant to the up to date safety management system in place, taking into account the requirements of the national PMSC document and the Guide to Good Practice for Marine Operations. This helps mitigate the risk that the BA PMSC is out of date and refers to non-existent and/or obsolete supporting documents.			Update: With the Marine Accident Investigation Branch (MAIB) investigation into Diamond Emblem 1 being delayed (draft report only available in Jan 2022) and the recent changes to the Hire Boat Code and Boat Safety Certification, the review of PMSC documentation deadline has been deferred until June 2022 to allow any recommendation from the MAIB to be incorporated in our safety systems. Completed.	Updated to 30/06/2022
7. Governance All relevant employees to be required to read and sign a copy of the PMSC on an annual basis. This assists in reducing the risk that employees are not familiar with the PMSC, leading to non-compliance with it.	Needs Attention	Head of Safety Management	Refresher training to be given at team meetings and attendance and signatures to be obtained. Update: Health & Safety Inductions for new starters now includes a PowerPoint presentation on PMSC/SMS this is also presented to new authority	By 31/10/2021 Updated to 31/12/22

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
			members. PMSC is a standard agenda item for the Safety Committee. Due to Covid-19 and safeguarding Operational we have had only one f2f full team meeting and other priority training was delivered at this time. The PMSC training will be delivered at the next Operational Technicians meeting in December 2022. Comment section updated and deadline extended to 31 December 2022.	

Appendix 4 – Summary of actions and responses to Internal Audit 2021/22

Table 5

HR and Payroll – December 2021

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
1. Staff Absences 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. This reduces the risk of inconsistent or ineffective resilience plans increase the risk of service failure in the event of staff absence.	Important	Directors	Agreed. Update: This has not been completed for all Directorates due to other priorities and staff shortages.	By 31/03/2022 Updated to 30/09/2022
2. Staff Absences The Business Continuity Plan be reviewed and updated. The review of the Business Continuity Plan is listed as an action on the risk register to mitigate the risk of loss of staff or expertise. Therefore, if the Business Continuity Plan is not updated, the staff loss risk remains higher.	Important	Directors	Agreed. Completed.	By 31/03/2022
3. Staff Absences Data on sickness absence rates be reported to senior management on a regular basis.	Important	Head of HR	Agreed. Completed.	By 31/03/2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
Without regular, consistent information, there is a risk that significant absence issues or trends will not be identified and addressed.				
4. Policies and procedures All HR policies be reviewed and updated to ensure that they are reflective of current arrangements and working practices. If policies are out of date, there is a risk of staff being given incorrect information or following outdated practices.	Needs Attention	Head of HR	Agreed. Initial review by 30/06/2022 and complete review by 31/12/2022.	By 31/12/2022

Table 6

Key Controls – February 2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
1. Treasury Management The Authority should consider diversifying its investment portfolio across different banking institutions. A lack of investment diversification could result in a loss of funds should the financial institution holding the investment fail.	Needs Attention	Director of Finance	Agreed. Update: Options are currently being explored however it should be noted that current investments require 95 days' notice before funds can be transferred to another institution.	By 31/07/2022

Table 7
Corporate Governance and Risk Management – May 2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
1. Risk Management The risks within the Corporate and Directorate Risk Registers be linked to the organisation's objectives. The risk is that the organisation is not clear on which objective(s) are at risk. By including links to objectives there will be better clarity of the risk and the wider impact, particularly where more than one objective is impacted.	Important	Senior Governance Officer	Management Team agreed on to add an additional column on both the CRR and DRRs to identify which objective(s) the risk related to. Completed see agenda item no. 12.	By 26/07/2022
2. 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. It is not clear that the Member has positively confirmed that they have no declarations of interest, or whether this was omitted accidentally. Results of backup testing must be used to inform and improve the process via lessons learned sessions.	Needs Attention	Senior Governance Officer	All member forms have been reviewed to ensure no blank fields. The form to be amended so that a response must be provided before the form can be submitted. Completed.	By 30/06/2022
3. 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.	Needs Attention	Senior Governance Officer	Management Team noted that risks such as cyber-crime were retained on the CRR, despite scoring below 16, as members	By 26/07/2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
The risk is that the Corporate Risk Register could become unnecessarily overloaded, and therefore lead to a lack of strategic focus.			had requested sight of these. Agreed to amend wording in policy paragraph 5.3 to say: "unless considered to be a Corporate Risk". Completed see agenda item no. 12.	
4. Risk Management Framework Management to include a target risk score within the risk registers. This practice provides assurance that risk actions are having the desired impact on the inherent score and therefore assists in mitigating the risk that risks are not being reduced in line and as expected with the mitigations in place.	Needs Attention	N/A	Disagreed. Management Team agreed that they did not consider this necessary as the aim was always to have as low as possible risk score, through the appropriate mitigation.	N/A
5. Risk Management Framework Management to undertake a Training Needs Assessment in respect of Risk Management and introduce Risk Management training if deemed necessary. This helps mitigate the risk that risks are not assessed in line with agreed policy and therefore practices may be applied incorrectly and/or inconsistently.	Needs Attention	Head of HR	Management Team agreed to amend the induction programme for new staff to include "To review and understand the Risk Management Policy" for all section heads. Completed.	By 01/06/2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
6. Risk Management Framework 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. This helps mitigate the risk that high risks are not highlighted as such to the Audit and Risk Committee and therefore the status of risks is unclear and misleading.	Needs Attention	N/A	Disagreed. This error was rectified upon notification. Management Team agreed 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.	N/A

Table 8
Maturity Assessment of Cyber Security – June 2022

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
1. Data Security 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.	Needs Attention	Head of ICT and Collector of Tolls	Agreed.	By 31/01/2023
2. Data Security	Needs Attention	Head of ICT and Collector of Tolls	Agreed.	By 31/01/2023

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
Results of backup testing must be used to inform and improve the process via lessons learned sessions.				
3. Incident Management 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.	Important	Head of ICT and Collector of Tolls	Agreed.	By 31/10/2022
4. Incident Management 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.	Important	Head of ICT and Collector of Tolls	Agreed.	By 31/10/2022
5. Incident Management 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.	Needs Attention	Head of ICT and Collector of Tolls	Agreed.	By 31/01/2023

Recommendations	Priority rating	Responsible Officer(s)	BA response/action	Timetable
6. Incident Management 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.	Needs Attention	Head of ICT and Collector of Tolls	Agreed.	By 31/01/2023