Appendix 1

Devon Audit Partnership

Draft Internal Audit Report

Torbay Council

Tor Bay Harbour Authority IT System Administration and Security

September 2012

Restricted

Devon Audit Partnership

The Devon Audit Partnership has been formed under a joint committee arrangement comprising of Plymouth, Torbay and Devon councils. We aim to be recognised as a high quality internal audit service in the public sector. We work with our partners by providing a professional internal audit service that will assist them in meeting their challenges, managing their risks and achieving their goals. In carrying out our work we are required to comply with the CIPFA code of practice for Internal Audit and other best practice and professional standards.

The partnership is committed to providing high quality, professional customer services to all; if you have any comments or suggestions on our service, processes or standards, the Head of Partnership would be pleased to receive them at Robert.hutchins@devonaudit.gov.uk

Confidentiality and Disclosure Clause

This report is protectively marked in accordance with the National Protective Marking Scheme. Its contents are confidential and, whilst it is accepted that issues raised may well need to be discussed with other officers within Torbay Council, the report itself should only be copied/circulated/disclosed to anyone outside of the organisation in line with the organisation’s disclosure policies.

This report is prepared for the organisation’s use. We can take no responsibility to any third party for any reliance they might place upon it.

1 Introduction

Torbay Council as a Harbour Authority operates and manages three enclosed harbours within the statutory harbour of Tor Bay. The statutory responsibilities of a Harbour Authority are considerable and include the provision of moorings and storage for various types of vessels.

A 5 year rolling audit plan was taken to the Harbour Committee and approved in June 2011 separating the various operation and strategic elements of the harbour operation into distinct audit areas; this audit is the second audit from the rolling plan and focuses on IT system administration security.

2 Audit Opinion

Improvements Required - In our opinion there are a number of instances where controls and procedures do not adequately mitigate the risks identified. Existing procedures need to be improved in order to ensure that they are fully reliable. Recommendations have been made to ensure that organisational objectives are not put at risk.

3 Executive Summary

The Harbour Authority utilises a number of IT systems and interfaces to assist with its day to day operation. These include the Harbour Management System (HMS), the weather station, the navigation lights system (PANAR), a visual system for tracking the movement of vessels within its waters (AIS), and the CCTV system. This audit has focussed mainly on the use of HMS, and has identified a number of weaknesses related both to the system's functionality, and knowledge of its use by Harbour officers.

There is no system documentation pertaining to the HMS system, and some officers are unaware of what the system can do, or how to use it properly. We have therefore been unable make an assessment in relation to how it could be used more appropriately or effectively, and have made recommendations that management should support officers in familiarising themselves with system and its capabilities.

The system does not have adequate controls in use to prevent and detect inaccurate data entry, access controls are weak and unenforceable, and there are issues with some of the relationships between items of data within the underlying database. Given these findings, management may wish to liaise with the Council's IT department, and consider whether they are willing to accept the risks associated with the lack of in built controls in these key areas, or whether manual controls could be introduced to mitigate them, before deciding on future system utilisation.

Issues have also been identified in relation to the use by the Harbour Authority of the Council's CCTV system, as there is no up to date guidance in place. This has resulted in the system being used inconsistently across the three offices and confusion over a number of processes and requirements. We understand that procedural documentation is currently revised by the Corporate CCTV team, however there should be liaison with Harbour management and the Information Governance team, before the document is finalised, and any updates should be clearly communicated to Harbour officers to ensure that risks in relation to data protection breaches are minimised.

The detailed findings and recommendations regarding these issues and less important matters are described in the Appendices. Recommendations have been categorised to aid prioritisation. Definitions of the priority categories the assurance opinion ratings are also given in the Appendices to this report.

4 Assurance Opinion on Specific Sections

The following table summarises our assurance opinions on each of the risks covered during the audit. These combine to provide the overall assurance opinion at Section 2. Definitions of the assurance opinion ratings can be found in the Appendices.

Risks Covered		Level of Assurance
1	Inappropriate use of IT systems	Fundamental weaknesses
2	Unauthorised / inappropriate access to the IT systems	Improvements Required
3	Data is not reliable	Improvements Required
4	Loss of data or assets	Improvements required
5	Inappropriate use of CCTV	Improvements required

The findings and recommendations in relation to each of these risks are discussed in the "Detailed Audit Observations and Action Plan" appendix. This appendix records the action plan agreed by management to enhance the internal control framework and mitigate identified risks where agreed. Management are required to agree an action plan, ideally within three weeks of receiving the draft internal audit report. Written responses should be returned to Carolyn Moody (carolyn.moody@devon.gov.uk) or Lynda Sharp-Woods (lynda.sharp-woods@devonaudit.gov.uk). Alternatively a meeting to discuss the report and agree the action plan should be arranged with the named auditors.

5 Issues for the Annual Governance Statement

The evidence obtained in internal audit reviews can identify issues in respect of risk management, systems and controls that may be relevant to the Annual Governance Statement.

In terms of this review, should the issues in relation to the use of the HMS system not be addressed quickly, we recommend that this be considered for reporting in the Annual Governance Statement at the end of the financial year.

6 Scope and Objectives

The audit scope has previously been agreed for 2012/13, as taken to Harbour Committee in June 2012; hence this audit is focussing on IT system administration and security and its associated controls.

This audit has been undertaken based on the following key risk areas bulleted below using previous audit work and input from Harbour staff to ensure that the programme is relevant to the organisation:

- Inappropriate use of IT systems
- Unauthorised / inappropriate access to the IT systems
- Data is not reliable
- Loss of data or assets
- Inappropriate use of CCTV

7 Inherent Limitations

The opinions and recommendations contained within this report are based on our examination of restricted samples of transactions / records and our discussions with officers responsible for the processes reviewed.

8 Acknowledgements

We would like to express our thanks and appreciation to all those who provided support and assistance during the course of this audit

.

Robert Hutchins
Head of Audit Partnership

Appendix B

Definitions of Audit Assurance Opinion Levels

Assurance	Definition
High Standard.	The system and controls in place adequately mitigate exposure to the risks identified. The system is being adhered to and substantial reliance can be placed upon the procedures in place. We have made only minor recommendations aimed at further enhancing already sound procedures.
Good Standard.	The systems and controls generally mitigate the risk identified but a few weaknesses have been identified and / or mitigating controls may not be fully applied. There are no significant matters arising from the audit and the recommendations made serve to strengthen what are mainly reliable procedures.
Improvements required.	In our opinion there are a number of instances where controls and procedures do not adequately mitigate the risks identified. Existing procedures need to be improved in order to ensure that they are fully reliable. Recommendations have been made to ensure that organisational objectives are not put at risk.
Fundamental Weaknesses Identified.	The risks identified are not being controlled and there is an increased likelihood that risks could occur. The matters arising from the audit are sufficiently significant to place doubt on the reliability of the procedures reviewed, to an extent that the objectives and / or resources of the Council may be at risk, and the ability to deliver the service may be adversely affected. Implementation of the recommendations made is a priority.

Definition of Recommendation Priority

Priority	Definitions
High	A significant finding. A key control is absent or is being compromised; if not acted upon this could result in high exposure to risk. Failure to address could result in internal or external responsibilities and obligations not being met.
Medium	Control arrangements not operating as required resulting in a moderate exposure to risk. This could result in minor disruption of service, undetected errors or inefficiencies in service provision. Important recommendations made to improve internal control arrangements and manage identified risks.
Low	Low risk issues, minor system compliance concerns or process inefficiencies where benefit would be gained from improving arrangements. Management should review, make changes if considered necessary or formally agree to accept the risks. These issues may be dealt with outside of the formal report during the course of the audit.

Confidentiality under the National Protective Marking Scheme

Marking	Definitions
Not Protectively Marked or Unclassified	Documents, information, data or artefacts that have been prepared for the general public or are for the public web pages or can be given to any member of the public without any exemptions or exceptions to release applying, have the classification NOT PROTECTIVELY MARKED. Some organisations will also use the word UNCLASSIFIED for publicly available information.
Protect	Any material that may cause distress to individuals, breach proper undertakings to maintain the confidence of information provided by third parties, breach statutory restrictions on the disclosure of information, cause financial loss or loss of earning potential, or to facilitate improper gain, give unfair advantage for individuals or companies, prejudice the investigation or facilitate the commission of crime, disadvantage government in commercial or policy negotiations with others should be marked PROTECT.
Restricted	Information or data or documents that should only be shared between a specific group of work staff who have to demonstrate a need to know, because of the sensitive content, then the document must be marked RESTRICTED.
Confidential	Material that is so sensitive that only specific named staff should have access. Special handling rules apply and so CONFIDENTIAL must only be applied to highly sensitive data.
Secret and Top Secret	Information with this sensitivity is unlikely to be available to the Partnership and the Chief Executive of the relevant organisation must make the decision to apply either of these protective markings. These markings are only to be used with information that can only be shared on a strict must know basis, with each party having signed a specific confidentiality agreement.