

Maldon District Council
INTERNAL AUDIT PROGRESS REPORT
November 2017



CONTENTS

Introduction	3
Definitions of assurance	4
Progress since August 2017 Committee	5
Progress Against 2017/18 Plan	6
Appendices:	
A: Executive Summary - Information Management (2017/18)	8
B: Executive Summary - Contracts Procurement Management and Purchasing (2017/18)	10

INTRODUCTION

Internal Audit

This report is intended to inform the Audit Committee of progress made against the 2017/18 internal audit plan which was approved by this Committee in March 2017. It summarises the work we have done, together with our assessment of the systems reviewed and the recommendations we have raised. Our work complies with Public Sector Internal Audit Standards. As part of our audit approach, we have agreed terms of reference for each piece of work with the risk owner, identifying the headline and sub-risks which have been covered as part of the assignment. This approach is designed to enable us to give assurance on the risk management and internal control processes in place to mitigate the risks identified.

Internal Audit Methodology

Our methodology is based on four assurance levels in respect of our overall conclusion as to the design and operational effectiveness of controls within the system reviewed. The assurance levels are set out in section 2 of this report, and are based on us giving either "substantial", "moderate", "limited" or "no". The four assurance levels are designed to ensure that the opinion given does not gravitate to a "satisfactory" or middle band grading. Under any system we are required to make a judgement when making our overall assessment. Our definitions are set out on page 4.

Work outside of the Internal Audit Plan

We are assisting with the provision of a Risk Management briefing to the Audit Committee in December 2017.

We will also be performing the Council's Annual Fraud Risk Assessment.

Audits Completed Since Last Report

See page 5 for details of the audits completed since the previous Audit Committee.

Overview of 2017/18 work to date

See pages 6 and 7 for a summary of the progress of 2017/18 planned work.

DEFINITIONS OF ASSURANCE

LEVEL OF ASSURANCE	DESIGN of internal control framework		OPERATIONAL EFFECTIVENESS of internal controls	
	Findings from review	Design Opinion	Findings from review	Effectiveness Opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non compliance and/or compliance with inadequate controls.

Recommendation Significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

PROGRESS SINCE AUGUST 2017 AUDIT COMMITTEE

Area	No. of days	Manager Responsible	Assurance - System Design	Assurance - Operating Effectiveness	No. of High priority recommendations	No. of Medium priority recommendations	No. of Low priority recommendations	Ref to Executive Summary
Information Management (Advisory review)	30	Simon Mitchell and Wendy Morse	N/A	N/A	0	7	0	Appendix II
Contracts Procurement Management and Purchasing	25	Carrie Cox	Moderate	Moderate	0	3	3	Appendix III

PROGRESS AGAINST 2017/18 PLAN

Area	2017/18 days	Date work to be undertaken	Progress Update	Assurance - System Design	Assurance - Operating Effectiveness
Core Audits					
Main Financial Systems	40	Q3	Draft Terms of Reference have been issued to the Council, pending management approval		
Budget Setting (High Level Review)	9	Q4	Draft Terms of Reference have been issued to the Council, pending management approval		
Policy Review	13	Q4	Timing agreed		
Counter Fraud	10	Q4	Fraud risk assessment		
	72				
Other Key Areas					
Economic Development / Business Rates growth	15	In progress	In Progress		
Attendance Management	10	Q4	Timing agreed		
Business Resilience	15	Q3	Draft Terms of Reference have been issued to the Council, pending management approval		
Contract Procurement Management and Purchasing	25	Draft report	Draft report issued 15 November	Moderate	Moderate
Partnership Working	15	Q3	Draft Terms of Reference have been issued to the Council, pending management approval		
Elections Improvement Plan (High level Review)	8	Q4	Scoping meeting scheduled for January 2018		
Information Management (Advisory review)	30	Draft report	Draft report issued 29 September	N/A	N/A
	118				

PROGRESS AGAINST 2017/18 PLAN

Area	2015/16 days	Date work to be undertaken	Progress Update	Assurance - System Design	Assurance - Operating Effectiveness
IT Audit					
Disaster Recovery and Business Continuity	15	Q3/Q4	Timing agreed		
	15				
Planning, Reporting, Follow-up and Contingency					
Planning / liaison / management	20	Ongoing			
Recommendation follow up	10	For reporting in September 2017 and March 2018	Reported in September 2017, further work is in progress and will be reported in March 2018		
Contingency	5	Q3	Risk Management briefing to the Audit Committee December 2017		
Total	35				

APPENDIX A - INFORMATION MANAGEMENT

CLIENT STRATEGIC RISKS		SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II FOR DEFINITIONS)	
Risk	The Council is not compliant with its statutory and regulatory obligations.	High	
ADVISORY REVIEW		Medium	7
The purpose of this work was to review the Council's systems and procedures for information management in light of the impending implementation of the General Data Protection Regulations (the GDPR) in May 2018 and to make recommendations as to how this can be improved to help the Council to make step changes in the way it uses information to assist in the transformation of the way the Council operates.		Low	
		Total number of recommendations: 7	
OVERVIEW			
<p>The use and management of information has a significant part to play in how the Council adapts and changes its services to meet the demands of its customers in the changing environment in which the Council operates. Furthermore, the transition from operating under the Data Protection Act 1998 (DPA) to the GDPR increases the risk of significant financial and reputational damage where the security of the Council's information is found to have been breached. The Council's Director of Resources, who is the Council's Senior Information Risk Owner (SIRO), is leading the GDPR compliance work.</p> <p>The purpose of this work was to review the Council's systems and procedures for information management in light of the impending implementation of the General Data Protection Regulations (the GDPR) in May 2018 and to make recommendations as to how this can be improved to help the Council to make step changes in the way it uses information to assist in the transformation of the way the Council operates.</p> <p>We found the following examples of good practice:</p> <ul style="list-style-type: none"> • The Council has defined the role for an Information Governance Officer and is actively recruiting for the role. • The Director of Resources will become the Council's Data Protection Officer as required by the GDPR. <p>However, we identified the following areas of improvement:</p> <ul style="list-style-type: none"> • There is not a defined programme in place to provide members of staff with appropriate information management training (Finding 1 - Medium) • The Council does not have a defined Information Asset Register in place (Finding 2 - Medium) • Existing ways of working that involve the use of personal identifiable information have not been reviewed for privacy issues (Finding 3 - Medium) • There are not standards in place for responding to requests from individuals under the GDPR (Finding 4 - Medium) • The Council does not have a defined, corporate Records Retention Schedule in place (Finding 5 - Medium) • Consideration has not been given to how the Council will obtain explicit consent from individuals for the processing of information (Finding 6 - Medium) • Information systems, which includes IT applications, have not been assessed in order to determine whether their operation is compliant with the requirements of the GDPR (Finding 7 - Medium). 			

APPENDIX A - INFORMATION MANAGEMENT

OVERVIEW (cont.)

In order to demonstrate compliance with the requirements of the GDPR with respects to the processing of information, the Council has to be able to demonstrate that its way of working incorporate both the consent of the individual and the privacy of their information. Whilst work has been undertaken to establish an information governance framework, there are a number of outstanding actions that will require co-operation from stakeholders from across the Council in order to implement. This review was requested by management, as GDPR is a new area and the Council required support to develop its approach. We have therefore treated it as an advisory audit and not provided an audit opinion on the current controls.

We have worked with the Council to prepare a GDPR programme of works that sets out the actions that will be completed in order to address the recommendations that have been raised within this report (see Appendix I). Working with the Legal and Democratic Services Manager and the IT Team Leader, we have prepared an indicative GDPR Programme Plan that is included within this report (see Appendix II). Furthermore, to support the Council in the identification and recording of its information assets, we have provided an example of an Information Asset Register (see Appendix III).

We propose a further audit is performed before May 2018 to ensure all recommendations have been implemented and at this point an opinion will be provided.

APPENDIX B - CONTRACTS PROCUREMENT MANAGEMENT AND PURCHASING

MALDON DISTRICT COUNCIL GOAL			SUMMARY OF RECOMMENDATIONS (SEE APPENDIX II FOR DEFINITIONS)	
Delivering good quality, cost effective and valued services			High	0
LEVEL OF ASSURANCE (SEE APPENDIX II FOR DEFINITIONS)			Medium	3
Design	Moderate	Generally sound system of internal controls, but with some exceptions	Low	3
Effectiveness	Moderate	Evidence of non compliance in some controls, that may put some system objectives at risk	Total number of recommendations: 6	

OVERVIEW

Background

The Council spends approximately £7 million on the procurement of goods, works and services, and has reviewed its Commissioning and Procurement Strategy and Contract Procedure Rules to ensure compliance with external requirements and to compliment corporate priorities. The Council's Facilities and Assets Manager, Procurement Officer and Finance Team provide guidance to staff and oversight of procurement related processes. The Council is also supported with delivery of procurement activity by the Essex Procurement Hub.

From our review, we noted the following areas of good practice, where the Council:

- has adopted a No PO No Pay protocol to ensure purchase orders are raised for expenditure
- works with the Essex Procurement Hub gaining access to dedicated expertise to support procurement activity
- has recently reviewed Financial Regulations and Contract Procedure Rules
- has provided training to Contract Managers in project management, to guide staff in procurement and contract related activity.

However, we also noted the following areas of improvement:

- Purchasing through one supplier exceeded thresholds for, but did not follow, required advertising or tendering requirements (Finding 1 - Medium)
- The Contracts Register was not up to date and did not reflect all Council Contracts (Finding 2 - Medium)
- Officers are using Purchase Cards for transactions that are of greater value that that expected by the Cardholder Instruction Manual (Finding 4 - Medium)

Conclusion

We have issued 3 Medium and 3 Low priority findings and have issued an opinion of moderate for both the design and effectiveness of the Contracts Procurement and Purchasing systems, reflecting that there are areas of good practice, but that there are also areas of improvement to be developed relating to compliance with procedures and regulations, and the provision of information and guidance to support compliance.

The proposal contained in this document is made by BDO LLP ("BDO") and is in all respects subject to the negotiation, agreement and signing of a specific contract. It contains information that is commercially sensitive to BDO, which is being disclosed to you in confidence and is not to be disclosed to any third party without the written consent of BDO. Client names and statistics quoted in this proposal include clients of BDO and BDO International.

BDO LLP, a UK limited liability partnership registered in England and Wales under number OC305127, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. A list of members' names is open to inspection at our registered office, 55 Baker Street, London W1U 7EU. BDO LLP is authorised and regulated by the Financial Conduct Authority to conduct investment business.

BDO is the brand name of the BDO network and for each of the BDO Member Firms.

BDO Northern Ireland, a partnership formed in and under the laws of Northern Ireland, is licensed to operate within the international BDO network of independent member firms.

Copyright ©2017 BDO LLP. All rights reserved.

www.bdo.co.uk