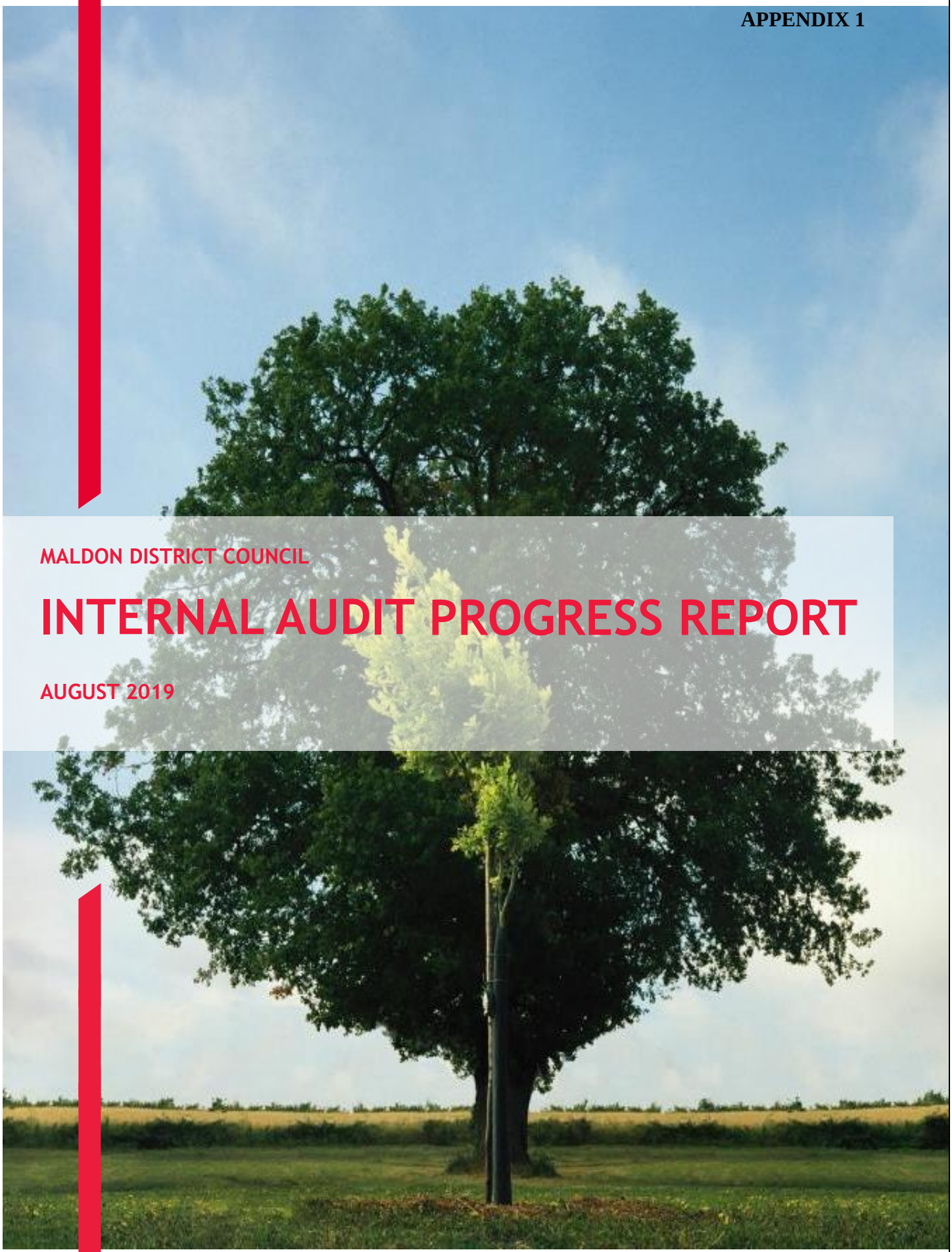
APPENDIX 1



MALDON DISTRICT COUNCIL

INTERNAL AUDIT PROGRESS REPORT

AUGUST 2019

BDO

CONTENTS

SUMMARY OF 2019/20 WORK

Internal Audit

This report is intended to inform the Audit Committee of progress made against the 2019/20 internal audit plan. 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 Appendix 1 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.

2018/19 Internal Audit Plan

The following audits have been issued in Final since the last audit committee:

- Local Development Plan
- Building Control (Appendix 2)

2019/20 Internal Audit Plan

The following audits have been issued in Final since the last audit committee:

- GDPR Compliance
- Risk Maturity Assessment (Appendix 3)

The following audit has been issued in draft since the last audit committee:

- Procurement and Contract Management

Reports for this Audit Committee

- Follow Up of Internal Audit Recommendations (Appendix 4)

REVIEW OF 2019/20 WORK

Audit Area	Audit Days	Planning	Fieldwork	Reporting	Opinion Design	Opinion Effectiveness
Audit 1. Main Financial Systems	20	✓				
Audit 2. Risk Maturity Assessment	15	✓	✓	August 2019	N/A	N/A
Audit 3. Corporate Governance	20	✓				
Audit 4. Workforce Management	15	✓				
Audit 5. Transformation Programme	25	✓				
Audit 6. GDPR Compliance	15	✓	✓	August 2019	Substantial	Moderate
Audit 7. IT Disaster Recovery	20	✓				
Audit 8. Procurement & Contract Management	15	✓	✓	Draft report issued		
Audit 9. Counter Fraud	10	✓				
Audit 10. Management of Property	15	✓				
Audit 11. Corporate Plan and Priorities	15	✓				
Audit 11. Commercialisation	15	✓				

APPENDIX A- DEFINITIONS

OPINION AND RECOMMENDATION SIGNIFICANCE DEFINITION

Level of Assurance	Design Opinion	Findings from review	Effectiveness Opinion	Findings from review
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.

APPENDIX B- GDPR COMPLIANCE

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)		
Design	Substantial	There is a sound system of internal control designed to achieve system objectives.
Effectiveness	Moderate	Evidence of non compliance with some controls, that may put some of the system objectives at risk.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I FOR DEFINITIONS)	
High	
Medium	3
Low	0

TOTAL NUMBER OF RECOMMENDATIONS: 3

BACKGROUND:

From May 25 2018, the General Data Protection Regulations (the GDPR) has replaced the Data Protection Act 1998 as the regulation governing the protection of data in the UK. As a data controller, the Council is obliged to comply with this new regulation and a programme of work is undertaken to implement the necessary governance framework.

The transition from operating under the Data Protection Act 1998 (DPA) to the GDPR increases the risk of significant financial and reputational damage should the security of the Council's information be found to have been breached.

The UK's withdrawal from the EU may also affect the 'legal obligation' lawful basis (which is under EU Member State law); hence following exit from the EU organisations may not be able to process EU citizens' personal data under this lawful basis by relying solely on UK law.

Our approach was to conduct interviews to establish the maturity of the ways of working for each of our areas of our maturity assessment. We then sought documentary evidence that these ways of working are designed as described. We evaluated these controls to identify whether they meet the maturity level assessed by the Council.

We sought to gain evidence of the satisfactory operation of the controls to verify the effectiveness of the control through use of a range of tools and techniques.

GOOD PRACTICE:

We identified the following areas of good practice from our fieldwork:

- The Council is registered with the Information Commissioner's Office (ICO) as a Tier 2 organisation and registration is valid until the 18 April 2020
- Data protection policy (March 2018) was approved by Finance & Corporate Services Committee and Council, and clearly sets responsibilities and security needs for all staff.
- Comprehensive retention schedule was also approved by Council and developed through consultation with all functions. It sets appropriate periods based on needs and legislation.
- Terms of reference for the newly formed Information Governance Board are in place, and stipulates: quorum, agenda and frequency.
- The Council's data protection officer (DPO) led the formation of an information sharing group with DPOs from other Essex Councils, which has proven to be effective.
- The DPO and previous Head of IT sourced subscription payments from finance and reconciled to applications to verify completeness of the information asset register.
- There are five processing streams which require consent to be obtained and recorded. Sample testing confirmed that adequate electronic records were held for all cases.
- Data security is listed as a key risk in the Resources' directorate's risk register and is regularly reviewed and updated by the Director of Resources.
- Subject access request (SAR) process was built from the FOI procedures. A template request form is available to the public, and a clear SAR manual has been developed.
- Only a total of six SARs have been received since May 2018. Sample testing confirmed complete responses were returned to subjects on average within 11 days of receipt.
- Council's terms and disclaimer webpage covers all requirements of the privacy notice as per ICO guidance: DPO contact details, types of personal data held, lawful basis for processing, how personal data is processed, and the rights of all data subjects.
- Total of three data breaches have occurred since May 2018 which the DPO holds a tracking worksheet for. Testing verified that all breaches were assessed (impact) and addressed (reported to ICO and necessary action taken) within one day.
- Training was rolled out in February (DPO) and March (online) 2018. Presentations were delivered by the DPO to all staff members, and 94% had completed the eLearning module by June 2018. The remaining users were addressed later in the year.

KEY FINDINGS:

We have also identified the following key areas of weakness which need addressing:

- Security controls, user access and the information asset register itself were last reviewed in June 2018 and need to be reviewed and updated on a regular basis going forwards (Finding 1)
- Data privacy impact assessments (DPIAs) need to be updated by data/system owners and built into the information asset register (Finding 2)
- Contractual addendums need to be reviewed and agreed with contractors where necessary and built into the information asset register (Finding 3)

CONCLUSION:

Overall, we conclude that the control framework in place for monitoring and managing compliance with GDPR is substantially designed and operationally effective to a moderate level but management need to address the areas of risk identified from this review.

MANAGEMENT ACTION PLAN

Ref	Recommendation	Management Response	Responsible Officer	Implementation date
1	a) All data sources and corresponding applications should be reviewed on at least an annual basis to ensure access risks, security measures and general changes are updated and managed. b) Management should consider holding an induction session with all assigned data owners following the staff restructure to ensure responsibilities are understood.	The issues and findings from this review were discussed and agreed with the data protection officer on the 13th June 2019	Emma Holmes	31 October 2019
2	Information Governance Group should provide oversight and ensure DPIAs are completed as soon as possible where necessary by responsible management (i.e. DPO and data owners).	The issues and findings from this review were discussed and agreed with the data protection officer on the 13th June 2019	Emma Holmes	31 December 2019
3	Information Governance Group should provide oversight and ensure contractual addendums are agreed as soon as possible where necessary by responsible management (i.e. contract owners).	The issues and findings from this review were discussed and agreed with the data protection officer on the 13th June 2019	Emma Holmes	31 September 2019

APPENDIX C- LOCAL DEVELOPMENT PLAN

LEVEL OF ASSURANCE: (SEE APPENDIX I FOR DEFINITIONS)		
Design	Moderate	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Moderate	Evidence of non compliance with some controls, that may put some of the system objectives at risk.

SUMMARY OF RECOMMENDATIONS: (SEE APPENDIX I FOR DEFINITIONS)	
High	0
Medium	2
Low	1

TOTAL NUMBER OF RECOMMENDATIONS: 3

BACKGROUND:

The Local Development Plan (LDP) sets out the planning strategy for future growth over the next 15 years. It is the means by which Maldon District Council will deliver sustainable development across the Maldon District and provides a spatial strategy for the delivery of the required future employment, homes, retail, community facilities and infrastructure provision. It has a number of component parts which sit alongside the spatial strategy. These include development management policies and strategic site allocations.

The Council published the Local Development Plan Preferred Options consultation document in July 2012 (MDC, 2012g). Following on from the Preferred Options consultation, the Council published the Draft Local Development Plan for consultation in August 2013 (MDC, 2013k). The consultation was undertaken for 6.5 weeks, and a consultation pack (a leaflet, a questionnaire and a return envelope) was sent to every household and business within the District. Over 3,600 responses were received.

The Pre-Submission LDP was consulted on in January-February 2014. Comments were invited on whether the Plan had been prepared in accordance with the duty to co-operate, legal and procedural requirements, and whether the Plan was 'sound'. Responses were received from over 220 people and organisations. Following this consultation the LDP was submitted to the Secretary of State for Examination-in-Public (EiP) on 25 April 2014. In May 2015 the Inspector issued his interim findings. He found that one policy H6 Provision for Travellers was unsound and therefore the whole plan was unsound.

On 8 March 2016 the Secretary of State restarted the Examination and appointed a new Inspector. In September to October 2016 a consultation was held on the Main Modifications to the LDP that had arisen from the previous Examination Hearings. The Inspector submits his report directly to the Secretary of State, who approved the Plan on 21 July 2017.

The Planning and Compulsory Purchase Act 2004, as amended by the Localism Act 2011, requires local planning authorities to prepare and maintain a Local Development Scheme (LDS). The purpose of the LDS is to set out the subject matter, area to be covered and timetable for

the preparation and revision of local development documents, including Supplementary Planning Documents (SPDs) and the Statement of Community Involvement (SCI).

In essence, it is a project plan setting out the timetable for work to be undertaken from February 2019 until January 2021. It sets out details of the documents that will be given priority during this period.

It is likely that the Council will not meet its five year housing land supply target, which will trigger an early review of the LDP. This is reflected in the Council's risk register.

GOOD PRACTICE:

We identified the following areas of good practice from our fieldwork:

- Risks related to the delivery of the LDP are on the Corporate Risk Register and discussed quarterly
- Significant public consultation has been undertaken on policies and plans to ensure stakeholder involvement
- The Local Development Scheme (LDS) has been developed and is in operation detailing upcoming documents and these are in the process of being established
- An efficient approach to production of the Authority Monitoring Report is in place through the use of Factsheets

KEY FINDINGS:

We have also identified the following key areas of weakness which need addressing:

- There is no formal monitoring of the day-to-day delivery in order to better track the numerous deadlines that stem for the LDP and LDS (**Finding 1 - Medium**)
- Mitigating actions for the risks relating to planning found on the Corporate Risk Register have implementation dates that are overdue or significantly in the future (**Finding 2 - Medium**)
- No consultation statement was developed and made available to the public following the public consultation for the LDP (Finding 3 – Low)

CONCLUSION:

Our review identified that the LDP process has been well managed with key requirements having been adhered to with a good understanding of work remaining. The LDS is in place and clearly identifies which policies and plans are intended in the year to come. However, there are findings relating to public awareness and the updating of risks, which has led to a final assessment of moderate assurance over the control design and moderate assurance over the control effectiveness.

MANAGEMENT ACTION PLAN

Ref	Recommendation	Management Response	Responsible Officer	Implementation date
1	Produce a RAG report/schedule which details plans and policies to be produced as well as their milestones in order to provide better oversight of progress	We will produce a RAG report in line with the timescales of the LDS and in addition to this	Georgina Button	January 2020

		reflect monitoring in the Authority Monitoring Report (AMR).		
2	Mitigating action completion dates should be reviewed as part of the quarterly update process to ensure they are appropriate and the actions are still relevant.	There is a corporate review of risk underway and we will review this as part of this piece of work.	Georgina Button	January 2020
3	The Council should ensure that consultation statements are completed for all future consultations and made available via the Council's website	The Council will ensure the consultation process requires a statement for every consultation. This is normal practice, however, for the Sept 2016 main modifications consultation – a statement may not have been completed. This is likely due to an oversight based on staffing and structure changes at the time. For the March 2017 main modifications consultation – it's worth noting that this was specifically undertaken by the Council on behalf of the Planning Inspector.	Georgina Button	July 2019

FOR MRE INFORMATION:

EMMA DONNELLY
Audit Manager, Public Sector
Ext.552904 (Internal)
020 78552904 (Direct Line)
07923030487 (Mobile)

emma.donnelly@bdo.co.uk