



Mid Sussex District Council - Internal Audit Progress Report

Audit Committee

15 November 2022

Issued 07 November 2022

Contents

01 Introduction	1
02 Current Progress	1
03 Follow-Ups	1
04 Other Matters	2
A1 Current Progress – 2022/23 Plan	3
A2 Cyber Security – Is your safety net strong enough?	4
A3 Definitions of Assurance	5
A4 Statement of Responsibility	6
Contacts	7

Disclaimer

This report (“Report”) was prepared by Mazars LLP at the request of Mid Sussex District Council (MSDC), and terms for the preparation and scope of the Report have been agreed with them. The matters raised in this Report are only those which came to our attention during our internal audit work. Whilst every care has been taken to ensure that the information provided in this Report is as accurate as possible, Internal Audit have only been able to base findings on the information and documentation provided and consequently, no complete guarantee can be given that this Report is necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required.

The Report was prepared solely for the use and benefit of MSDC, and to the fullest extent permitted by law, Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification. Accordingly, any reliance placed on the Report, its contents, conclusions, any extract, reinterpretation, amendment and/or modification by any third party is entirely at their own risk. Further details are provided in Appendix A4, “Statement of Responsibility”.

01 Introduction

This report provides a summary of internal audit activity at Mid Sussex District Council (MSDC) since the last Audit Committee (Committee), including:

- An update on progress in delivering the 2022/23 internal audit plan;
- A summary of any Limited/Unsatisfactory Assurance reports issued and high-priority recommendations raised; and
- An update on follow-up activity and any recommendations outstanding for implementation.

The Committee approved the 2022/23 Internal Audit Plan (Plan) on 20 September 2022. The Plan was developed by applying a risk-based approach to provide Members, management, and other external bodies with independent assurance on the adequacy of the Council's risk management, governance, and internal control framework.

02 Current Progress

Since the last Committee, we have resourced the audits included in the Plan and agreed on start dates with the relevant Services within the Council. For this reporting period, there is one audit with the fieldwork completed (**Business Rates**) and one due to start on 14 November 2022 (**Disabled Facilities Grants (DFG)**).

The Committee will recall the phasing of work in the prior year's plan, which saw the majority of audits commence in Q4 due to the timing of our appointment. Compared to our position reported in November last year, there is an improvement in progress, with more work planned to start in Q3 this year. Also, our last planned audit is due to start in March 2023. This should allow us to complete the fieldwork for all audits in the Plan before April 2023.

Since the last meeting of the Committee, the following progress has been made:

Reports issued

- We have issued our final report for the 2021/22 **Cyber Security** audit, in which we raised 13 recommendations (which includes three high-priority recommendations). We understand Mid Sussex are linking these recommendations with their LGA and Cabinet Office Cyber 360 review.
- Although our **IT Audit Needs Assessment** report was issued as a draft in August 2022, we are waiting for final responses and confirmation from Management before we issue a final version. We have been working in partnership to agree the specific actions and timescales that are appropriate to Mid Sussex. We expect to issue a final report before the end of the calendar year.

Work in progress

At the time of drafting this report for the 2022/23 plan:

- We have completed fieldwork on the **Business Rates** audit. The draft report is at the final stages of the review process.
- The **DFG** audit will commence on 14 November 2022.

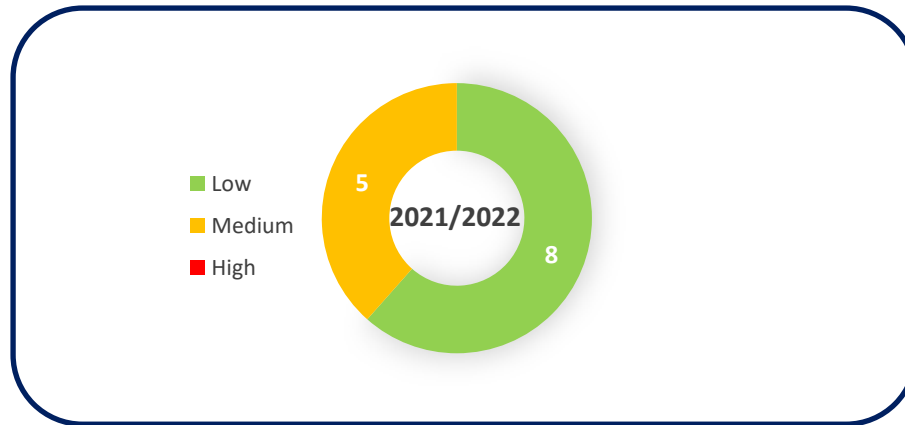
Further details of the Plan timetable and current status are detailed in Appendix A1.

03 Follow-Ups

In the delivery of our work last year, we included relevant recommendations raised by the former Internal Auditor from their 2020/21 Internal Audit reports. Also, we monitored recommendations raised as part of the 2021/22 internal audits and created a centralised record capturing these, including agreed management actions and timescales for implementation. This has been used as the basis of our follow-up activity.

As of 04 November 2022, there are 13 recommendations which have past their initially agreed implementation dates. There are a further 19 recommendations that were raised but are still within the agreed timescales

for implementation and, therefore, not reviewed. Priorities for overdue recommendations are as follows:



We will review these as part of cyclical work in 2022/23 (where applicable). We will discuss updates with the Director of Resources and Organisational Development and subsequently to this Committee in due course, including any outstanding high-priority actions (i.e., actions past their agreed implementation date). Also, we will liaise with the responsible Officers for implementing these.

04 Other Matters

At Mazars, we support the public sector by providing solutions and services that help organisations meet their challenges. We are committed to providing the insight and innovation that helps make informed decisions and deliver objectives.

In the most recent September 2022 Committee Meeting, the Chair requested Internal Audit to provide guidance on “what Internal Audit expects from the Committee and its Members”. In June 2021, we hosted a discussion forum for local authority Audit Committee Members, in which our team considered the role and purpose of an Audit Committee. This was

followed by a panel discussion, in which Mazars experts were joined by Audit Committee members from two London boroughs.

We aim to hold another forum in November 2022, and further details about joining this session will be shared with the Chair and Members in due course. If you would like any more information on the webinar or would like to take part in the next session, please get in touch with us.

[Audit Committee webinar for local authorities - Mazars - United Kingdom.](#)

Also, Mazars has issued a survey report titled ‘Cyber Security– Is your safety net strong enough?’. This report takes as its starting point the inevitability of being cyber-attacked. Cyber security is no longer a question of if but when. That may amount to a mindset shift for many business leaders, but we believe it’s an important one to make. Further detail is included in Appendix A2.

A1 Current Progress – 2022/23 Plan

Audit area	Progress	Assurance Opinion	Recommendations		
			High	Medium	Low
Business Rates	Fieldwork Complete.	-	-	-	-
DFG	Starts 14/11/2022	-	-	-	-
Data Protection Act / Freedom of Information	Starts 09/01/2023	-	-	-	-
Accounts Payable (Creditors)	Starts 30/01/2023	-	-	-	-
Financial Management System	Starts 08/02/2023	-	-	-	-
Commercial & Investment Property Portfolio	Starts 13/02/2023	-	-	-	-
Accounts Receivable (Debtors)	Starts 17/02/2023	-	-	-	-
HR – Recruitment and Retention	Starts 20/02/2023	-	-	-	-
Building Controls	Starts 13/03/2023	-	-	-	-
NFI – Data Matching	Reports/matches expected in Q4	-	-	-	-
IT					
IT Disaster Recovery	Starts in Q4	-	-	-	-
Data Security	Starts in Q4	-	-	-	-
Total			0	0	0

A2 Cyber Security – Is your safety net strong enough?

Cyber threats are all around us. This is not paranoia, it's an unfortunate reality: every day brings new hacks, new data leaks, new embarrassment – and new costs, both financial and commercial. Nobody is spared. The attacks target large and small companies, public-sector institutions, and individuals. How can organisations protect themselves?

The cyber dangers that lurk in the shadows for private-sector companies are no less of a threat to national and local government and other public sector organisations — and in some ways more so. The data these organisations hold is often intensely private and confidential, ranging from social security details and tax filings to education information and health and criminal justice records.

Our annual survey of more than 1,000 C-suite executives worldwide, conducted at the end of 2021, reveals that cyber security is now a major preoccupation among corporate leaders. Effective cyber defence has become a delicate balancing act for many businesses; having a strong safety net that can cushion any eventual fall is paramount.

The report is available to download via the link below.

Cyber security
**Is your safety net strong
enough?**

Discover the report



A3 Definitions of Assurance

Definitions of Assurance Levels	
Level	Description
Substantial	The framework of governance, risk management and control is adequate and effective.
Moderate	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
Unsatisfactory	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

Definitions of Recommendations		
Priority	Definition	Action required
High (Fundamental)	Significant weakness in governance, risk management and control that, if unresolved, exposes the organisation to an unacceptable level of residual risk.	Remedial action must be taken urgently and within an agreed timescale.
Medium (Significant)	Weakness in governance, risk management and control that, if unresolved, exposes the organisation to a high level of residual risk.	Remedial action should be taken at the earliest opportunity and within an agreed timescale.
Low (Housekeeping)	Scope for improvement in governance, risk management and control.	Remedial action should be prioritised and undertaken within an agreed timescale.

A4 Statement of Responsibility

We take responsibility to MSDC for this report which is prepared on the basis of the limitations set out below.

The responsibility for designing and maintaining a sound system of internal control and the prevention and detection of fraud and other irregularities rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy and effectiveness of the system of internal control arrangements implemented by management and perform sample testing on those controls in the period under review with a view to providing an opinion on the extent to which risks in this area are managed.

We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify any circumstances of fraud or irregularity. Even sound systems of internal control can only provide reasonable and not absolute assurance and may not be proof against collusive fraud.

The matters raised in this report are only those which came to our attention during the course of our work and are not necessarily a comprehensive statement of all the weaknesses that exist or all improvements that might be made.

Recommendations for improvements should be assessed by you for their full impact before they are implemented. The performance of our work is not and should not be taken as a substitute for management's responsibilities for the application of sound management practices.

This report is confidential and must not be disclosed to any third party or reproduced in whole or in part without our prior written consent. To the fullest extent permitted by law Mazars LLP accepts no responsibility and disclaims all liability to any third party who purports to use or rely for any reason whatsoever on the Report, its contents, conclusions, any extract, reinterpreted amendment and/or modification by any third party is entirely at their own risk

Contacts

Graeme Clarke

Partner, Mazars

graeme.clarke@mazars.co.uk

Juan Fosco

Manager, Mazars

juan.fosco@mazars.co.uk

Mazars is an internationally integrated partnership specialising in audit, accountancy, advisory, tax and legal services*. Operating in over 90 countries and territories worldwide, we draw on the expertise of 44,000 professionals – 28,000 in Mazars' integrated partnership and 16,000 via the Mazars North America Alliance – to assist clients of all sizes at every stage in their development.

*where permitted under applicable country laws.

www.mazars.co.uk