East Herts Council
Audit and Governance Committee

19 July 2022
Shared Internal Audit Service –
Progress Report

Recommendation

Members are recommended to:
a) Note the Internal Audit Progress Report
b) Note the Status of Critical and High Priority Recommendations

Contents

1 Introduction and Background

<u>Purpose of Report</u>

1.1   To provide Members with:
    a) The progress made by the Shared Internal Audit Service (SIAS) in delivering the Council's 2022/23 Internal Audit Plan to 1 July 2022.
    b) The findings for the period 1 April 2022 to 1 July 2022.
    c) Details of any changes required to the approved Internal Audit Plan.
    d) The implementation status of previously agreed audit recommendations.
    e) An update on performance management information to 1 July 2022.

<u>Background</u>

1.2   Internal Audit's Annual Plan for 2022/23 was approved by the Audit and Governance Committee at its meeting on 5 April 2022. The Audit and Governance Committee receive periodic updates against the Internal Audit Plan. This is the first update report for 2022/23.

1.3   The work of Internal Audit is required to be reported to a Member Body so that the Council has an opportunity to review and monitor an essential component of corporate governance and gain assurance that its internal audit function is fulfilling its statutory obligations. It is considered good practice that progress reports also include proposed changes to the agreed Annual Internal Audit Plan.

2 Audit Plan Update

<u>Delivery of Internal Audit Plan and Key Audit Findings</u>

2.1   As of 1 July 2022, 20% of the 2022/23 Internal Audit Plan days have been delivered (the calculation excludes contingency days that have not yet been allocated).

2.2   The following final reports have been issued since the last Progress Report to the Audit and Governance Committee:

Audit Title	Date of Issue	Assurance Level	Number of Recommendations
Payroll (Assurance Mapping) 2021/22	May 2022	Reasonable	Two Medium and Three Low Priority
Main Accounting (Assurance Mapping) 2021/22	June 2022	Substantial	One Low Priority
Contain Outbreak Management Fund (Grant Audit) 2022/23	June 2022	Unqualified	None
Asset Management (Assurance Mapping) 2022/23	July 2022	Substantial	One Medium Priority

2.3 The table below summarises the position regarding delivery of the 2022/23 approved projects to 1 July 2022. Appendix A provides a status update on each individual project within the 2022/23 Internal Audit Plan.

Status	No. of Audits at this Stage	% of Total Audits
Final Report Issued	2	8%
Draft Report Issued	0	0%
In Fieldwork/Quality Review	3	13%
In Planning/Terms of Reference Issued	2	8%
Allocated	6	25%
Not Yet Allocated	11	46%
Cancelled/Deferred	0	0%
Total	**24**	**100%**

Proposed Internal Audit Plan Changes

2.4 There has been no amendment to the Internal Audit Plan since it was approved in April 2022.

Critical and High Priority Recommendations

2.5 Members will be aware that a Final Audit Report is issued when it has been agreed ("signed off") by management; this includes an agreement to implement the recommendations that have been made.

2.6 The schedule attached at Appendix B details any outstanding Critical and High priority audit recommendations. No new Critical or High Priority recommendations have been added to the schedule.

Performance Management

2.7 The 2022/23 annual performance indicators were approved at the SIAS Board meeting in March 2022.

2.8 The actual performance for East Herts Council against the targets that can be monitored in year is set out in the table below:

Performance Indicator	Annual Target	Profiled Target	Actual to 1 July 2022
1. Internal Audit Annual Plan Report – approved by the March Audit & Governance Committee or	Yes	N/A	Yes

the first meeting of the financial year should a March committee not meet			
2. Annual Internal Audit Plan Delivery – the percentage of the Annual Internal Audit Plan delivered (excludes contingency)	95%	24% (59/245)	20% (49/245)
3. Project Delivery – the number of projects delivered to draft report stage against projects in the approved Annual Internal Audit Plan	95%	17% (4/24)	8% (2/24)
4. Client Satisfaction – percentage of client satisfaction questionnaires returned at 'satisfactory' level	100%	100%	100% (1 received) Note (1)
5. Chief Audit Executive's Annual Assurance Opinion and Report – presented at the first Audit & Governance Committee meeting of the financial year	Yes	N/A	Yes

Note (1) – 1 received in 2022/23, this relating to a 2021/22 audit where the final report was issued after 1st April 2022.

2022/23 Internal Audit Plan

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
Key Financial Systems – 43 days Provision for full or targeted audit of one or more key financial systems. Mapping the remaining key financial systems to confirm appropriate lines of assurance and to inform the annual assurance opinion									
Business Rates (shared with SBC)						43	No	10	Not Yet Allocated
Council Tax (shared with SBC)							No		Not Yet Allocated
Housing Benefits (shared with SBC)							No		Not Yet allocated
Treasury Management (assurance mapping refresh only)							No		Not Yet Allocated
Debtors (assurance mapping refresh only)							No		Not Yet Allocated
Creditors (assurance mapping refresh only)							No		Not Yet Allocated
Payroll (assurance mapping refresh only)							No		Not Yet Allocated
Asset Management (assurance mapping)	Substantial	0	0	1	0		Yes		Final Report Issued
Main Accounting (assurance mapping refresh only)							No		Not Yet Allocated
Operational Audits – 51 days									
Contract Management						15	Yes	1	ToR Issued
Community Wellbeing & Partnerships						10	Yes	5	In Fieldwork
Housing Acquisition & Conversion – Queens Road						10	No	0	Not Yet Allocated
General Fund Health & Safety Property Compliance						10	No	0	Allocated
Refuse Services (shared with NHDC)						6	Yes	0	Allocated
Certifications - 5 days									
Contain Outbreak Management Fund	Unqualified	0	0	0	0	1	Yes	1	Complete
Contingency	N/A	-	-	-	-	4	No	0	Through Year
Corporate Services/Themes – 76 days									

APPENDIX A - PROGRESS AGAINST THE 2022/23 INTERNAL AUDIT PLAN

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
Transforming East Herts						20	No	0	Not Yet Allocated
Supply Chain Interruption						10	Yes	0.5	In Planning
Elections Payroll						10	Yes	0	Allocated
Customer Services						10	Yes	4	In Fieldwork
Information Governance						10	Yes	0	Allocated
Risk Management (assurance mapping refresh only)						3	No	0	Not Yet Allocated
Corporate Governance (assurance mapping refresh only)						3	No	0	Not Yet Allocated
Whistleblowing						10	Yes	5	In Fieldwork
IT Audits – 10 days									
Malicious Software (shared with SBC)						7	Yes	0	Allocated
Cyber Security (assurance mapping refresh only, shared with SBC)						3	Yes	0	Allocated
Shared Learning and Joint Reviews – 5 days									
Joint Review(s) – Topics to be confirmed by SIAS Board						5	No	0	Not Yet Allocated
Completion of 2021/22 Projects – 6 days									
Various						6	Yes	6	Complete
Contingency – 5 days									
Contingency						5	N/A	0	Through Year
Strategic Support – 49 days									
Head of Internal Audit Assurance Opinion 2021/22						3	Yes	3	Complete
Audit Committee & Recommendations Follow Up						12	Yes	3	Through Year
Client Meetings & Ad hoc Advice						10	Yes	2.5	Through Year

APPENDIX A - PROGRESS AGAINST THE 2022/23 INTERNAL AUDIT PLAN

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
Plan Monitoring, Work Allocation and Scheduling						12	Yes	3	Through Year
SIAS Development						5	Yes	5	Through Year
Matters Arising: Shared Anti-Fraud Service						2	Yes	0	Through Year
Audit Planning 2023/24						5	Yes	0	Through Year
EHC TOTAL		**0**	**0**	**1**	**0**	**250**		**49**	

The following appendix provides Audit and Governance Committee Members with a summary of the most recent update provided by management in respect of outstanding high priority recommendations.

No.	Report Title	Recommendation / Original Management Response	Responsible Officer / Original Due Date	Latest management update (or previous commentary where appropriate)	Status of Progress (July 2022)
1.	**Payment Card Data Security Standard (2020/21).**	<u>Recommendation:</u> <u>PCI-DSS Self-Assessment & Compliance Structure.</u> The Council has not completed a SAQ and does not have a formal PCI-DSS compliance strategy/program in place to meet required data security standards. As the option for non-compliance was taken several years ago and since that point there have been multiple personnel changes, the Council should re-assess the level of risk and decide if the non-compliant route is still the most preferred option. A cross-Council PCI-DSS working group should be established to focus on assessing the level of risk presented by sustained non-compliance with the PCI-DSS. This group's primary objective should be to determine whether to accept the level of risk and continue to pay the monthly penalty imposed by WorldPay or agree roles and responsibilities to engineer and maintain compliance with the published standards. Should the decision be made to focus on compliance, the Councils are recommended to consult the best practice guidance produced by the PCI DSS Council in January 2019. <u>Agreed Management Action(s):</u> The s.151 officer has advised that the level of risk and the monthly fines for non-compliance does not represent proper management of financial affairs. In addition, the expansion of the number of services to be put on the web, which require the ability to have payment facilities, means that the Council must be PCIDSS compliant in order to proceed. Having previous experience of ICON it is not possible to achieve PCIDSS compliance with this software and suitable replacement software has been identified. This will be implemented jointly with Stevenage BC. A revised Information Security Policy has been developed and will be distributed to staff annually as part of the compliance process. This emphasises card security measures in the short term.	**Responsible Officer:** Head of Strategic Finance & Property. **Due Date:** 31 March 2022.	<u>July 2022.</u> Verbal update to be provided at the meeting.	Partially implemented.

No.	Report Title	Recommendation / Original Management Response	Responsible Officer / Original Due Date	Latest management update (or previous commentary where appropriate)	Status of Progress (July 2022)
2.	**Payment Card Data Security Standard (2020/21).**	<u>Recommendation:</u> <u>Roles and Responsibilities.</u> As a subsequent output from the formation of the cross-Council PCI-DSS working group, there should be named individuals assigned to steering the Councils compliance journey. Traditionally, the ownership of the compliance process may be the Head of Finance, as they generally occupy the position of signing off the annual Attestation of Compliance (AoC). But it must also be noted that much of the compliance structure content relates to technical configuration, so the Council should designate roles based on this dual ownership. Whilst Finance owns the overall compliance objective, the IT work stream owns the infrastructure that the payment systems sit on. Both departments should have an equal vested interest in compliance. <u>Agreed Management Action(s):</u> The above will lead the new system implementation and compliance as he has done this at a previous authority. To achieve compliance the new system will not permit card number entry by staff. Instead, customers choosing to phone up to pay will be handed off to a secure IVR system and will need to enter card details on their phone keypad. Subsequent payments, providing it is for a service with an account number for the customer, e.g. Council Tax, then the system uses a secure token that shows the last 4 digits of the card number and the expiry date. The customer is asked to confirm the expiry date and payment can be taken from that card with no need for card input unless the card is replaced/renewed. About 60% of PCIDSS compliance relates to firewalls, encryption and network security and requires best practice testing and maintenance which will be usefully checked for PCIDSS compliance as well as the standard annual cyber security checks.	**Responsible Officer:** Head of Strategic Finance & Property. **Due Date:** 31 March 2022.	<u>July 2022.</u> Verbal update to be provided at the meeting.	Partially implemented.

APPENDIX C – INTERNAL AUDIT PLAN 2022/23 – INDICATIVE AUDIT START DATES AGREED WITH MANAGEMENT

EAST HERTS					
Apr	**May**	**Jun**	**July**	**Aug**	**Sept**
Customer Services In Fieldwork	Contract Management Terms of Reference Issued	Community Wellbeing & Partnerships In Fieldwork	General Fund Health & Safety Property Compliance Allocated	Refuse Services Allocated	Supply Chain Interruption In Planning
Information Governance Allocated	Whistleblowing In Fieldwork	Asset Management Assurance Mapping Final Report Issued		Elections Payroll Allocated	Malicious Software Allocated
		Contain Outbreak Management Fund Final Report Issued			
Oct	**Nov**	**Dec**	**Jan**	**Feb**	**Mar**
Housing Benefits Not Yet Allocated	Council Tax Not Yet Allocated	Creditors Assurance Mapping Refresh Not Yet Allocated	Corporate Governance Assurance Mapping Refresh Not Yet Allocated	Housing Acquisition & Conversion – Queens Road Not Yet Allocated	
	Business Rates Not Yet Allocated	Debtors Assurance Mapping Refresh Not Yet Allocated	Risk Management Assurance Mapping Refresh Not Yet Allocated	Cyber Security Assurance Mapping Refresh Allocated	
		Treasury Management Assurance Mapping Refresh Not Yet Allocated	Payroll Assurance Mapping Refresh Not Yet Allocated	Main Accounting Assurance Mapping Refresh Not Yet Allocated	

APPENDIX D – ASSURANCE / PRIORITY LEVELS

Audit Opinions	
Assurance Level	**Definition**
Assurance Reviews	
Substantial	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Not Assessed	This opinion is used in relation to consultancy or embedded assurance activities, where the nature of the work is to provide support and advice to management and is not of a sufficient depth to provide an opinion on the adequacy of governance or internal control arrangements. Recommendations will however be made where required to support system or process improvements.
Grant / Funding Certification Reviews	
Unqualified	No material matters have been identified in relation the eligibility, accounting and expenditure associated with the funding received that would cause SIAS to believe that the related funding conditions have not been met.
Qualified	Except for the matters identified within the audit report, the eligibility, accounting and expenditure associated with the funding received meets the requirements of the funding conditions.
Disclaimer Opinion	Based on the limitations indicated within the report, SIAS are unable to provide an opinion in relation to the Council's compliance with the eligibility, accounting and expenditure requirements contained within the funding conditions.
Adverse Opinion	Based on the significance of the matters included within the report, the Council have not complied with the funding conditions associated with the funding received.

Recommendation Priority Levels		
Priority Level		**Definition**
Corporate	**Critical**	Audit findings which, in the present state, represent a serious risk to the organisation as a whole, i.e. reputation, financial resources and / or compliance with regulations. Management action to implement the appropriate controls is required immediately.
Service	**High**	Audit findings indicate a serious weakness or breakdown in control environment, which, if untreated by management intervention, is highly likely to put achievement of core service objectives at risk. Remedial action is required urgently.
	Medium	Audit findings which, if not treated by appropriate management action, are likely to put achievement of some of the core service objectives at risk. Remedial action is required in a timely manner.
	Low	Audit findings indicate opportunities to implement good or best practice, which, if adopted, will enhance the control environment. The appropriate solution should be implemented as soon as is practically possible.