



East Herts Council  
Audit and Governance Committee

29 July 2021  
Shared Internal Audit Service –  
Progress Report

Recommendation

Members are recommended to:

- a) Note the Internal Audit Progress Report
- b) Approve Changes to the Internal Audit Plan as at 9 July 2021
- c) Note the Status of Critical and High Priority Recommendations

## Contents

- 1 Introduction and Background
  - 1.1 Purpose
  - 1.2 Background
  
- 2 Audit Plan Update
  - 2.1 Delivery of Audit Plan and Key Findings
  - 2.4 Proposed Audit Plan Changes
  - 2.5 Critical and High Priority Recommendations
  - 2.7 Performance Management

### Appendices:

- A Progress against the 2021/22 Audit Plan
- B Implementation Status of Critical and High Priority Recommendations
- C Audit Plan Items (April 2021 to March 2022) - Indicative start dates agreed with management
- D Assurance Definitions / Priority Levels

# 1 Introduction and Background

## Purpose of Report

- 1.1 To provide Members with:
- The progress made by the Shared Internal Audit Service (SIAS) in delivering the Council's 2021/22 Internal Audit Plan as at 9 July 2021.
  - The findings for the period 1 April 2021 to 9 July 2021.
  - Details of changes required to the approved Internal Audit Plan.
  - The implementation status of previously agreed audit recommendations.
  - An update on performance management information as at 9 July 2021.

## Background

- 1.2 Internal Audit's Annual Plan for 2021/22 was approved by the Audit and Governance Committee at its meeting on 16 March 2021. The Audit and Governance Committee receive periodic updates against the Internal Audit Plan. This is the first update report for 2021/22.
- 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

## Delivery of Audit Plan and Key Audit Findings

- 2.1 As at 9 July 2021, 17% of the 2021/22 Audit Plan days have been delivered (the calculation excludes contingency days that have not yet been allocated).
- 2.2 The following final report has been issued since the last Audit and Governance Committee:

Audit Title	Date of Issue	Assurance Level	Number of Recommendations
Fly Tipping	July 2021	Reasonable	Five Medium and Two Low priority

- 2.3 The table below summarises the position regarding 2021/22 projects as at 9 July 2021. Appendix A provides a status update on each individual project within the 2021/22 Internal Audit Plan.

Status	No. of Audits at this Stage	% of Total Audits
Final Report Issued	1	5

---

Draft Report Issued	1	5
In Fieldwork/Quality Review	0	0
In Planning/Terms of Reference Issued	6	32
Allocated	1	5
Not Yet Allocated	8	42
Cancelled/Deferred	2	11
<b>Total</b>	<b>19</b>	<b>100</b>

### Proposed Audit Plan Changes

- 2.4 The following Audit Plan changes were agreed with management and are proposed to the Committee:
- Corporate Capacity (12 days) – audit intended for quarter 1 but now deferred to 2022/23 after discussions with the Head of Human Resources and Organisational Development. It was considered that this revised timing is more appropriate acknowledging anticipated organisational change during 2021/22.
  - Audit Follow Up 1 (6 days) – audit intended for quarter 1 but now cancelled. Prudent provision for two follow up audits was made when the audit work programme was originally drafted in December 2020 (one in quarter 1 and a second in quarter 3). The first of these is not required.
  - Homes England: Compliance Audit (5 days) – new audit added for quarter 2. The Council has been selected for audit by Homes England, who require independent confirmation that all requirements and grant funding conditions have been complied with. It has been agreed with the Head of Housing & Health and Homes England that SIAS will provide the confirmation required.

Unused audit days have been returned to the contingency balance (now 16 days) for use later in the year.

### 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.

### Performance Management

- 2.7 The 2021/22 annual performance indicators were approved at the SIAS Board meeting in March 2021.
-

- 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 9 July 2021
<b>1. Planned Days</b> – percentage of actual billable days against planned chargeable days completed	95%	17% (49/284 days)	17% (47/284 days)
<b>2. Planned Projects</b> – percentage of actual completed projects to draft report stage against planned completed projects	95%	12% (2/17 projects)	12% (2/17 projects)
<b>3. Client Satisfaction</b> – percentage of client satisfaction questionnaires returned at 'satisfactory' level	100%	100%	100% (1 received) Note (1)
<b>4. Number of Critical and High Priority Audit Recommendations agreed</b>	95%	95%	No Critical or High Priority recommendations made/agreed to date

Note (1) – 1 received in 2021/22 relates to a 2020/21 audit.

## APPENDIX A - PROGRESS AGAINST THE 2021/22 INTERNAL AUDIT PLAN

### 2021/22 SIAS Audit Plan

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
<b>Key Financial Systems – 70 days</b>									
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						70	Yes	0.5	In Planning
<b>Operational Audits – 127 days</b>									
Resources Benefits Realisation						12	No	0	Not Yet Allocated
Capital Programme Delivery						12	No	0	Not Yet Allocated
Corporate Capacity						1	N/A	1	Cancelled
Contract Management						10	Yes	2.5	In Planning
COVID-19 Pandemic Response						12	Yes	0.5	In Planning
Fly-Tipping	Reasonable	0	0	5	2	11	Yes	11	Final Report Issued
Property Investment						10	Yes	0.5	In Planning
Licensed Premises						10	No	0	Not Yet Allocated
Economic Development						12	No	0	Not Yet Allocated
Equalities						12	Yes	11.5	Draft Report Issued
Safeguarding						10	Yes	1.5	In Planning
Temporary Accommodation/Rough Sleepers						10	No	0	Not Yet Allocated
Homes England – compliance audit						5	Yes	0	Allocated
<b>Follow Up Audits – 6 days</b>									
Follow Up 1						0	N/A	0	Cancelled
Follow Up 2						6	No	0	Not Yet Allocated

**APPENDIX A - PROGRESS AGAINST THE 2021/22 INTERNAL AUDIT PLAN**

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
<b>Risk Management and Governance – 12 days</b>									
Provision for full or targeted audits or mapping the lines of assurance to inform the annual assurance opinion						12	No	0	Not Yet Allocated
<b>IT Audits – 16 days</b>									
IT Resilience						6	No	0	Not Yet Allocated
Cyber Security Assurance Mapping						10	Yes	0.5	In Planning
<b>Shared Learning and Joint Reviews – 6 days</b>									
Joint Review(s) – Topics to be confirmed by SIAS Board						6	No	0	Not Yet Allocated
<b>Follow Up of Audit Recommendations – 4 days</b>									
Follow up of critical and high priority audit recommendations						4	Yes	0.5	Through Year
<b>Completion of 2020/21 Projects – 3 days</b>									
Various						3	Yes	3	Complete
<b>Contingency – 16 days</b>									
Contingency						16	N/A	0	Through Year
<b>Strategic Support – 40 days</b>									
Head of Internal Audit Assurance Opinion 2020/21						3	Yes	3	Complete
External Audit Liaison						1	Yes	0	Through Year
Audit Committee						8	Yes	2	Through Year
Client Meetings & Ad hoc Advice						7	Yes	1.5	Through Year
Plan Monitoring, Work Allocation and Scheduling						12	Yes	2.5	Through Year
SIAS Development/External Quality						5	Yes	5	In Progress

**APPENDIX A - PROGRESS AGAINST THE 2021/22 INTERNAL AUDIT PLAN**

---

AUDITABLE AREA	LEVEL OF ASSURANCE	RECS				AUDIT PLAN DAYS	LEAD AUDITOR ASSIGNED	BILLABLE DAYS COMPLETED	STATUS/COMMENT
		C	H	M	LA				
Assessment									
Audit Planning 2022/23						4	Yes	0	Through Year
<b>EHC TOTAL</b>		<b>0</b>	<b>0</b>	<b>5</b>	<b>2</b>	<b>300</b>		<b>47</b>	

---



**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
1.	Cyber Security follow up (2018/19).	<p><u>Network access control.</u> Management should establish a network access control to block unknown or unauthorised devices from connecting to the Council's IT network. This should include restricting the ability to physically connect to the IT network.</p> <p>Where there is a demonstrable need for a device to connect to the IT network, the Service should require:</p> <p>The purpose for the connection has been recorded</p> <p>Appropriate security controls have been enabled on the device connecting to the IT network</p> <p>The period of time that the device will require the connection</p> <p>All connections are approved before being allowed to proceed.</p> <p>Devices connected to the IT network should be reviewed on a routine basis.</p>	The Council has created a Security & Network Team who has been tasked to look at security / network tools. There is also a planned upgraded Office 365 and in particular Intune to manage all mobile (non-network connected) devices. The plan is to ensure that only known devices are allowed to access Council systems.	ICT Strategic Partnership Manager.	Network Tools July 2019. Intune October 2019. Procurement of network tools revised to November 2020.	<p><u>July 2019.</u> This is a new addition and the management response opposite is therefore the latest comment.</p> <p><u>September 2019.</u> Intune MDM has been installed and will be rolled out to manage all mobile devices and Windows 10 laptops. Plan in place to upgrade all Laptops to windows 10 is in place to ensure control via Intune encryption using Bitlocker.</p> <p>Financial and resource restrictions have forced the procurement of network tools to financial year 2020/21.</p> <p><u>December 2019.</u> Revised date as above. It is very rare (if ever) that someone connects an external device to the IT network. The Zero Clients do not allow the transfer of data to anything plugged into it.</p> <p><u>February 2020.</u> Revised implementation date as above.</p>	With the exception of the network monitoring tool (scheduled Q3), the original recommendation has been implemented.

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
						<p><u>July 2020.</u> Budget obtained to purchase networking tools to cover this and other security areas. The procurement will start shortly.</p> <p><u>December 2020.</u> Project has a dependency on completion of the networking/Firewall upgrade. As any tools need to be able to work within those systems capabilities. The Networking project is at the end of the procurement phase but has come under some procurement and technical issues which are holding up implementation.</p> <p><u>February 2021.</u> Access remotely: Our VDI Hosted desktop solution gives good security controls over who can access our systems. This will be strengthened with the installation of an upgraded system this year which will force Multi Factor authentication. Access via our buildings WiFi: This security is enforced as above, stopping any access.</p>	

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
						<p>Physical access: Due to current lockdown and the decision to focus on our network and hosted desktop upgrade, the project to purchase network monitoring tools has been put on hold. The ability to access our system by plugging in a device to our system is reduced by our hosted desktop solution, as this is inaccessible without authentication. The tool to monitor and restrict physical access is scheduled for Q3 2021.</p> <p><u>July 2021.</u> No change from the above scheduled position for Q3 2021.</p>	
2.	Incident Management follow up (2018/19).	<p><u>Updating the disaster recovery plan.</u> Management should update the Council's IT disaster recovery plan to include the procedure for establishing all IT services at a single data centre. A complete IT Disaster Recovery scenario test on all applications and systems should take place to provide assurance that recovery could happen within the expected time</p>	With our upgrade to horizon VDI, we are installing hardware which will allow either site to run 100% of capacity allowing the complete downing of one site for upgrade work but will of course allow for full capacity in the event on one data centre being of offline.	ICT Strategic Partnership Manager.	August 2019 – DR review. April 2020 - VDI upgrade.	<p><u>July 2019.</u> This is a new addition and the management response opposite is therefore the latest comment.</p> <p><u>September 2019.</u> VDI upgrade out to tender with award scheduled for October 2019.</p> <p><u>December 2019.</u> Expected completion for this work is now April 2020.</p>	Partially implemented – continue to monitor.

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
		<p>frame. The Service should document the results of the test to determine the further actions required to improve the efficacy of the plan.</p>				<p><u>February 2020.</u> As above.</p> <p><u>December 2020.</u> Project dependant on upgrade of infrastructure as above.</p> <p>However limited pilot has been started and work on preparing applications is underway.</p> <p>£5,000 has been obtained from Local Government funding source by SBC to train 2 staff on DR planning.</p> <p><u>February 2021</u> ICT has a solid incident management response procedure, but this is not fully documented into a recognised Disaster Recovery Plan due to the changes being made to our systems and network. Any plan created now will be out of date in a few months, hence the delay.</p> <p><u>July 2021.</u> No change from the above scheduled position for Q3 2021.</p>	

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
3.	Payment Card Data Security Standard (2020/21).	<p><u>PCI-DSS Self-Assessment &amp; Compliance Structure.</u></p> <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>	<p>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.</p> <p>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.</p>	Head of Strategic Finance & Property.	31 March 2022.	<p><u>July 2021.</u></p> <p>This is a new addition and the management response opposite is therefore the latest comment.</p>	Not yet implemented – continue to monitor.

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
		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.					
4.	Payment Card Data Security Standard (2020/21).	<p><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.</p> <p>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.</p> <p>Whilst Finance owns the overall compliance objective, the IT work stream owns the</p>	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	Head of Strategic Finance & Property.	31 March 2022.	<p><u>July 2021.</u> This is a new addition and the management response opposite is therefore the latest comment.</p>	Not yet implemented – continue to monitor.

**APPENDIX B – IMPLEMENTATION STATUS OF CRITICAL AND HIGH PRIORITY RECOMMENDATIONS**

No.	Report Title	Recommendation	Management Response	Responsible Officer	Implementation Date	History of Management Comments	SIAS Comment (July 2021)
		<p>infrastructure that the payment systems sit on. Both departments should have an equal vested interest in compliance.</p>	<p>taken from that card with no need for card input unless the card is replaced/renewed.</p> <p>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.</p>				





**APPENDIX C – AUDIT PLAN ITEMS (APRIL 2021 TO MARCH 2022) – INDICATIVE START DATES AGREED WITH MANAGEMENT**

Quarter 1	Quarter 2	Quarter 3	Quarter 4
Corporate Capacity Cancelled	Contract Management In Planning	Key Financial Systems In Planning	Key Financial Systems In Planning
Fly Tipping Draft Report Issued	COVID-19 Pandemic Response Allocated	Resources Benefits Realisation Not Yet Allocated	Licensed Premises Not Yet Allocated
Equalities Draft Report Issued	Property Investment In Planning	Capital Programme Delivery Not Yet Allocated	Temporary Accommodation / Rough Sleepers Not Yet Allocated
Audit Follow Up 1 Cancelled	Safeguarding In Planning	Economic Development Not Yet Allocated	Risk Management & Corporate Governance Not Yet Allocated
	Cyber Security In Planning	Audit Follow Up 2 Not Yet Allocated	IT Resilience Not Yet Allocated
	Homes England – Compliance Audit Allocated		



## APPENDIX D – ASSURANCE / PRIORITY LEVELS

Assurance Level	Definition
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.

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 / Advisory		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.